

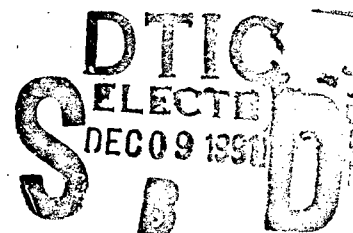
AD-A243 119



20000831231

NAVAL POSTGRADUATE SCHOOL

Monterey, California



THESIS

HUMAN FACTORS IN NETWORK SECURITY

by

Francis B. Jones

March, 1991

Thesis Advisor:

Tung X. Bui

Approved for public release; distribution is unlimited

Reproduced From
Best Available Copy

91-17296



91 12 0 043

Unclassified
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE				
1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED		1b. RESTRICTIVE MARKINGS		
2a. SECURITY CLASSIFICATION AUTHORITY		3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.		
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE				
4. PERFORMING ORGANIZATION REPORT NUMBER(S)		5. MONITORING ORGANIZATION REPORT NUMBER(S)		
6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b. OFFICE SYMBOL (if applicable) 037	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School		
6c. ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000		7b. ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000		
8a. NAME OF FUNDING/SPONSORING ORGANIZATION	8b. OFFICE SYMBOL (if applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER		
3c. ADDRESS (City, State, and ZIP Code)		10. SOURCE OF FUNDING NUMBERS		
		Program Element No.	Project No.	Task No. Work Unit Accession Number
11. TITLE (Include Security Classification) Human Factors in Network Security				
12. PERSONAL AUTHOR(S) Jones, Francis B., LT, USN				
13a. TYPE OF REPORT Master's Thesis	13b. TIME COVERED From To	14. DATE OF REPORT (year, month, day) 1991, March 21	15. PAGE COUNT 110	
16. SUPPLEMENTARY NOTATION The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
17. COSAT CODES		18. SUBJECT TERMS (continue on reverse if necessary and identify by block number)		
FIELD	GROUP	SUBGROUP		
			Human Factors, Network, Security	
19. ABSTRACT (continue on reverse if necessary and identify by block number) Human factors, such as ethics and education, are important factors in network information security. This thesis determines which human factors have significant influence on network security. Those factors are examined in relation to current security devices and procedures. Methods are introduced to evaluate security effectiveness by incorporating the appropriate human factors into network security controls.				
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS REPORT <input type="checkbox"/> DTIC USERS		21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED		
22a. NAME OF RESPONSIBLE INDIVIDUAL T. X. Bui		22b. TELEPHONE (Include Area code) 646-2630		22c. OFFICE SYMBOL AS/Bd

DD FORM 1473, 84 MAR

83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

Approved for public release; distribution is unlimited.

Human Factors in Network Security

by

Francis B. Jones
Lieutenant, United States Navy
B.S., United States Naval Academy, 1983

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS


from the

NAVAL POSTGRADUATE SCHOOL
March, 1991


Author:


Francis B. Jones

Approved by:


T. X. Bui, Thesis Advisor


R. L. Knight, Second Reader


D. R. Whipple, Chairman
Department of Administrative Science

ABSTRACT

Human factors, such as ethics and education, are important factors in network information security. This thesis determines which human factors have significant influence on network security. Those factors are examined in relation to current security devices and procedures. Methods are introduced to evaluate security effectiveness by incorporating the appropriate human factors into network security controls.

Accession For	
NTIS GRA&I	<input checked="checked" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By _____	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	



TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	BACKGROUND.....	1
B.	OBJECTIVES.....	2
C.	RESEARCH QUESTION.....	2
D.	SCOPE, LIMITATIONS AND ASSUMPTIONS.....	2
E.	ORGANIZATION OF STUDY.....	3
II.	ISSUES IN HUMAN FACTORS SECURITY.....	4
A.	SECURITY CONCERNS.....	4
B.	HUMAN FACTORS.....	6
1.	Ethics.....	6
2.	Education.....	9
C.	SOLUTIONS.....	11
D.	NETWORK SECURITY IN THE DOD.....	14
E.	SUMMARY.....	15
III.	NETWORK DATA DAMAGE AND SECURITY DEVICES.....	17
A.	INTRODUCTION.....	17
B.	POTENTIAL SYSTEM DAMAGE.....	17
1.	Destruction or contamination.....	17
2.	Theft or disclosure.....	18
3.	Modification.....	18
4.	Interruption or denial of service.....	19
5.	Resources used in eliminating intruders.....	19
6.	Public embarrassment.....	19

C.	ACCESS CONTROLS.....	20
1.	Passwords.....	21
2.	Passphrases.....	26
3.	Token.....	27
4.	Dial-back devices.....	28
5.	Diskless workstations.....	29
D.	BIOMETRIC ACCESS CONTROLS.....	29
1.	Signature verifier.....	30
2.	Retinal scanners.....	30
3.	Fingerprint scanners.....	31
4.	Voiceprint.....	32
5.	Hand Geometry.....	32
E.	SUMMARY.....	33
IV.	NETWORK SECURITY PROCEDURES.....	34
A.	INTRODUCTION.....	34
B.	SECURITY ENHANCING PROCEDURES.....	35
1.	Password associated procedures.....	35
a.	Passphrases.....	36
b.	Password ageing.....	36
c.	Password generation.....	37
d.	Password monitor.....	38
2.	Auditing.....	38
3.	Concept of "Least Privilege".....	40
4.	Independence of control and subject.....	40
5.	Separation of duties.....	41
6.	Universal application.....	41

7. Defensive depth.....	42
8. Least common mechanism.....	44
9. Default to denial.....	45
10. Dial-up access.....	46
C. RISK ANALYSIS PROCEDURES.....	46
1. Checklists.....	46
2. Quantitative risk evaluation.....	47
3. Scenario-based method.....	47
4. Qualitative risk analysis.....	48
D. SUMMARY.....	48
V. FACTORS AFFECTING SECURITY MOTIVATION.....	50
A. INTRODUCTION.....	50
B. DEMOTIVATING FACTORS.....	51
1. Security control forced upon user.....	51
2. Control takes a long time to perform.....	52
3. Control interferes with user's routine.....	52
4. Control is invasive.....	54
5. Management not committed to controls.....	55
C. MOTIVATING FACTORS.....	56
1. Involvement in the control process.....	56
2. Personal responsibility for controls.....	57
3. Reward users for good security practices....	58
4. Easy, fast, and accurate controls.....	59
5. Users are comfortable with controls.....	59
6. Management support of security controls.....	60
D. HUMAN FACTORS IN SPECIFIC SECURITY CONTROLS.....	60

E.	SECURITY OPTIMIZATION.....	61
1.	Using the optimization grid.....	63
2.	Grid divisions.....	64
F.	SUMMARY.....	65
VI.	ENHANCING SECURITY CONTROLS: A HUMAN FACTORS PERSPECTIVE.....	66
A.	INTRODUCTION.....	66
B.	EVALUATING THE CURRENT SYSTEM.....	67
C.	BUILDING SUPPORT FOR IMPROVEMENT.....	69
1.	Management support.....	69
a.	Security plan.....	71
b.	Selling the plan.....	74
2.	User support.....	77
a.	Ethics program.....	77
b.	System involvement.....	79
c.	Training.....	81
D.	SYSTEM IMPROVEMENT.....	83
1.	Organizational strategies.....	83
2.	Workplace strategies.....	85
3.	Personnel strategies.....	87
E.	MAINTAINING SECURITY.....	88
1.	Employee accession.....	89
2.	Hiring agreements.....	90
3.	Job descriptions.....	91
4.	Punishment.....	91
5.	Functional cooperation.....	91

6. System personalization.....	92
7. System review.....	92
F. SUMMARY.....	93
VII. CONCLUSIONS, RECOMMENDATIONS AND SUGGESTIONS FOR FUTURE RESEARCH.....	94
A. CONCLUSIONS.....	94
B. RECOMMENDATIONS.....	95
C. SUGGESTIONS FOR KEY RESEARCH.....	96
LIST OF REFERENCES.....	98
BIBLIOGRAPHY.....	100
INITIAL DISTRIBUTION LIST.....	101

I. INTRODUCTION

A. BACKGROUND

Networks have greatly increased the utility of computer systems, allowing multiple users in diverse geographic positions to share scarce or unique resources. The same factors that make networks desirable, however, also increase their risks and vulnerabilities. The ease with which network resources can be accessed from many entry points raises concerns about unauthorized access, disclosure, or modification of data by unauthorized personnel.

Most effort put forth in the field of network security focuses on the technical aspects of security controls. A neglected aspect of network security is the effect that human factors, such as user acceptance of controls, management support, and the ethical environment of the organization, have on the effectiveness of the controls in place.

Given that no hardware or software controls can function efficiently without the support of those who work with them, the area of human factors in network security controls is important to the overall understanding and enhancement of security controls in a networked information system environment.

B. OBJECTIVES

This thesis will identify the issues that are important in a discussion of network security human factors. It will examine security devices and procedures that are currently in use, and explore the way human factors affect their functionality. The factors that influence security motivations will be considered, and methods to enhance network security controls using these factors will be developed.

C. RESEARCH QUESTION

The primary research question of this thesis is: What are the human factors that affect network security? A subsidiary question is: How can a security manager utilize these factors to enhance security in his/her organization?

D. SCOPE, LIMITATIONS AND ASSUMPTIONS

The scope of this thesis includes only those security controls that have a noticeable effect on the user. Controls such as end-to-end encryption of data is of course a network security control, but it is transparent to the user, and thus will not be addressed. Only controls noticeable by the user are relevant to this subject.

Limitations of the research effort are the lack of significant prior inquiry into the subject. Materials used in the research were widely scattered about the literature of computer security, psychology, and human engineering.

Assumptions made in this work are that the reader has a working familiarity with computers, in particular the potential problems associated with network access to information.

E. ORGANIZATION OF STUDY

The remaining chapters of this thesis examine the pertinent issues in human factors security, and discuss how these factors affect currently used security devices and procedures. Factors that influence the users security motivations and environment are then considered. Finally, a capstone chapter synthesizes the security controls with the human element in a methodology to enhance an organization's network security.

II. ISSUES IN HUMAN FACTORS SECURITY

A. SECURITY CONCERNS

Concerns for safeguarding information in networks generates tremendous interest in computer security in the United States. The average computer-related theft is estimated at between \$400,000 and \$600,000 (Sobol, 1983). U.S. sales of physical computer security equipment will reach 4.1 billion by 1993, up 33% from 1986 (Klopp, 1990). The fact that this data is available suggests the importance it holds for business. There is no comparable data available for the dollars spent on developing new security procedures, or educating users in security methods. There is no data available even on the amount of losses as compared with ADP expenditures. This information is lacking because many organizations disregard these aspects of security completely, and others give them only token acknowledgement.

Computer security in modern networked information systems is crucial to the acceptance and growth of electronic networks in the future. Besides the financial costs mentioned, two other factors stimulate interest in network data security. These are; extensive telecommunications systems binding networks together, and the concern for individual and corporate privacy that networks threaten to erode. Wide use

of teleprocessing systems, leading inevitably to the handling of sensitive data, generates concern for many reasons.

For example, data communication networks are used for elaborate message systems such as electronic mail. These e-mail systems transmit information between office systems on a large scale. Much of the information carried is sensitive and needs protection against eavesdropping. Another example is the use of data networks for transmitting and authorizing payments. These messages must be authenticated and protected from tampering, to prevent fraudulent alteration.

The second interest-stimulating factor is concern about privacy of the individual user. There is a threat to this privacy in the handling of personal information in computer systems. Electronic privacy law is beginning to operate in technically advanced countries. Such laws require that personal information is safeguarded, and accessed only with proper authorization. In network applications, sensitive information should be secured against wrongful access.

In many organizations, access to this sensitive information is less restricted than in the past, due to the decentralization of data that networks allow. Data that previously was centrally controlled has migrated onto desktop computers. Personnel information, financial data, or even proprietary business information might reside on a desktop computer used by one or more employees. This information, if not protected, is accessible by any computer-literate person

who happens by. A security system is necessary to protect the information of the organization and its employees.

Security has business benefits as well. It has the expected advantages of information integrity. A good security system also greatly reduces the normal administrative and operational misuse of system resources.

B. HUMAN FACTORS

1. Ethics

The field of ethics focuses on our relations with others and their property. Information technology creates new and unfamiliar relationships. The concepts of property and ownership take on different meanings when applied to information rather than to tangible property.

For example, if you have a car, and someone takes it, you no longer have a car; you are deprived of the possession and use of your property. However, if you have some information stored in electronic media, and someone copies it, you still have possession and use of the information. This is an area where our societal ethics are still being developed, since the problem has only been around for a relatively short time.

Sorting out the priorities between the right to know versus the right to privacy is another difficult task. Our basic drive with respect to property is to accumulate and protect, but for information, it is to communicate and to

share. Thus, information protection can run counter to our fundamental traits.

It is difficult to modify these traits when there exists a general lack of "informational ethics" role models within the computer world. Organizations to which people normally look for ethical leadership, such as church, school, government, and home, currently lack the technical knowledge, budget, or the awareness to deal with the subject as it applies to the present electronic world. Normally accepted role models are not present for informational ethics.

Security efforts can be sorted into three areas; technological, organizational, and behavioral. The technical approaches are many, and have an excess of supporters and vendors to keep us aware. Organizational security efforts involve compartmentalization of information and restriction of knowledge. Greater degrees of compartmentalization yield greater security, but can subtract from the company's efficiency and effectiveness. For this reason, profit-motivated entities are prone to rely less on this method than on technology.

The behavioral methods seem to have attracted little attention. Perhaps this is true because it is easy to focus on technological advances, of which there is a great supply. It is much more difficult, sometimes impossible, to modify behavior and attitudes. Figure 1a shows how technology and organization are commonly used as the only inputs to security

in a system. Figure 1b is the way human behavioral factors actually influence security by acting on the two primary inputs. This influence must be acknowledged and incorporated into any integrated security effort.

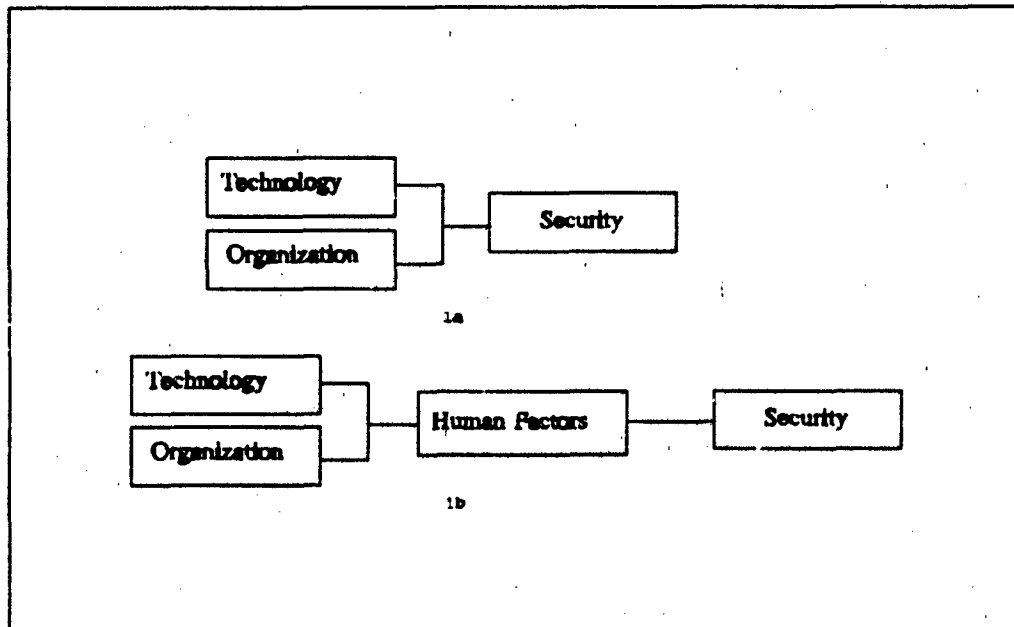


Figure 1. (a) Current View, (b) Human Factors Influence

Technological security devices, hardware and software based, can be tremendous aids in securing computer networks. Without vigilant human beings, however, the value of security technology is severely limited. If no one reviews the login audit files, or responds to intruder alert alarms, even the best security devices are useless. Without a well-trained and highly motivated staff, the computer system simply cannot work efficiently. When technology has done its best, human factors must be the focus of network security efforts.

Security of information is just as dependant on the user accepting his security responsibilities as it is on the data security officer doing his job. By involving human factors, though, security systems design and implementation becomes extremely complex and confusing.

A primary contributor to the confusion is the lack of a clearly defined code of ethics for the "Electronic Information Age". Electronically stored and transmitted information makes our existing ethical codes difficult to apply clearly and consistently, for many reasons.

In this climate of ambiguous informational ethics, network security practitioners should understand that focusing on the human aspects of security can yield far greater benefits than concentrating on the machine aspects.

2. Education

Computer security personnel have long been aware of the danger of malicious remote threat, but have not often addressed it as a major problem. This is because other issues, such as programming and hardware errors, data entry errors, and software maintenance overshadow the remote access issue.¹

Security problems often take a back seat to other organizational problems, because common wisdom says that security violations are rare occurrences. Priority is thus given usually to other matters. A better measure of the need

¹On a network, all access can be considered "remote access".

for good security practices than the number of incidents is the potential impact of a single incident.

In today's complex networked environment, one person could theoretically disrupt a major financial, transportation, manufacturing, or public service network. In the case of a medical information system, this may even cause loss of life. This problem transcends simple security consciousness and goes back to the previously discussed importance of ethical principles.

Destruction of information is the most obvious of all penetrations. Its effects can range from the inconvenience of having to restore data from backup tapes, to bringing a business to a halt if the information is not backed up.

With unauthorized modification of information, the risks are considerably higher. The modification may not be detected until it is too late, if at all. Meanwhile, the organization may have made decisions using the modified data as if it were accurate.

Unauthorized retrieval of information is the most difficult to detect. The information is not missing, nor is it changed, but its unauthorized dissemination has the potential of a far more serious impact than the other two possibilities.

Until the security issue is seen as equally important, and given a priority at least equal to the day to day maintenance of networks, information systems will be exposed

to more potential risk through misuse of data than these other issues of data entry and program errors offer altogether.

The beginnings of a trend in the correct direction is emerging as more computer-literate people enter the workforce. Many more are capable now of understanding and manipulating non-secure systems. This makes potential problems more likely, thus security will receive more attention.

C. SOLUTIONS

When protecting a network's security, managers must be aware of who are potential intruders. Users of information can be intruders. Providers, or the developers of information systems, can be intruders. Servicers of the system can be intruders. Emphasis is usually assigned to protect against the outside intruder or the hacker. This emphasis is misplaced. The potential intruders inside the organization are far more dangerous than the random hacker. The people who commit computer crimes most frequently are legitimate users of the system (Zimmerman, 1984).

To protect against these malicious users, designers of networks need to know three things about the people who will use the system. First, what are their abilities and skills? This refers to their technical knowledge and abilities. If your users are sophisticated and knowledgeable, the system must be designed with sophisticated and current defenses.

Second, what are their inabilities? An example is the inability of most people to remember random passwords without writing them down. The designer should be aware of this inability so that it may not be exploited against the system.

Third, the designer must know what the users will want to do, what their motivations are. If the users are programmers, they will likely be more curious, and likely to challenge the system than data entry personnel. Procedures should be set up to curb this curiosity, or provide outlets for it that will not compromise the system.

In any system where people are involved, security procedures must address the human aspects. People in our society are not usually security oriented. People make errors; people commit crimes; and people are vulnerable to bribery and threats.

For example, how often have you seen remote access terminal rooms with account numbers and passwords written on blackboards in the room. Or well-secured computer facilities -- with the side door propped open so employees can get some fresh air. Or people using coded identification cards to pass through secured gates -- and then holding the gate open for another person.

These are common, well-accepted everyday habits of ordinary people. Unfortunately, they are precisely the types of behavior that give security officers headaches. Because it is impossible to change human nature, the human element must

be realistically factored into any security system. As long as human beings are a functional part of a computer security system, the system is unavoidably vulnerable to the physical and moral weaknesses contained in the human makeup.

The responsibility of security professionals is to convince the people who use computers that they should be concerned about security. The path to enlightenment is a dangerous one, though. In making computer systems secure, users must usually adopt or conform to practices to which they are unused. They may resent these, and this will likely slow down their use of the system.

In creating secure computing environments, we must avoid appearing to propose a "Red Flag Act".² Security procedures need to be developed that users are comfortable with, and with which they feel it is in their own interest to comply.

To develop effective and appropriate security procedures, involvement is required at all levels. Concerned users, experienced technical specialists, and others with appropriate security knowledge must cooperate during all phases of system development. Those who know how to incorporate security controls into systems have to take the lead in setting a security-receptive development environment.

²When the automobile was first introduced into Great Britain, it brought with it the unfortunate phenomena of traffic fatalities. In response, the government introduced a law requiring all cars to be preceded by a man on foot waving a red flag. Although greatly increasing safety, this act had the effect of limiting the auto to the speed of a walking man. (Haigh, 1984)

Included in the required levels of involvement is upper management. Just as with any program in an organization, management support is required for a security program to be effective. Management needs to be involved in the security process. They are the people who authorize and fund security programs, and their attitude toward system security sets the tone for the organizational attitude.

D. NETWORK SECURITY IN THE DOD

Computer security in the Federal Government is addressed by the Computer Security Act of 1987, which mandates "periodic training for all persons who manage, use, or operate Federal computer systems containing sensitive information." (US Congress, 1987) Unfortunately, the generalities of the Act have not led to many specific guidelines for information system security.

The Department of the Navy, however, recognizes that the proliferation of ADP systems in the military brings with it special security concerns related to network environments (Department of the Navy, 1988). It sets out guidelines for risk management and sets minimum requirements for physical security, but has no specific procedures to follow. It merely assigns responsibility for program development, and defines the terms introduced in the instruction itself.

SECNAVNOTE 5230, the ADP Control Guidelines, comes closer to addressing human factors issues (Secretary of the Navy,

1988). It discusses setting computer security policies, segregation of duties in a network environment, and the need for training programs. Specific methods for allowing access to terminals, reviewing user lists, and classifying data are also included. This instruction is the most useful of those available in addressing human factor issues of security, yet it falls far short of being comprehensive, or even detailed enough to do more than set general guidelines.

The reason for this dearth of network security documents is that this is a new area of responsibility for the military. The Federal government only recognized the issue in 1987. The services have thus had only 3 years to begin programs. The current state of network security programs in the military is one of overall policy statements, general responsibilities, and the beginnings of training requirements.

E. SUMMARY

This chapter has detailed the human factor issues surrounding network security. Interest in network security is motivated by people's need for privacy. That the need for privacy directly contradicts our societal attitude toward sharing information creates a difficult and complex problem. To solve this problem, efforts must focus on its causes, human needs and motivations. Only with this focus will the technology-oriented security devices in use be able to

function effectively. The next chapters will examine these devices, and current security procedures that attempt to address these issues.

III. NETWORK DATA DAMAGE AND SECURITY DEVICES

A. INTRODUCTION

This chapter introduces the types of damage that can occur in a system, describes various security devices that are currently available, and discusses the strengths and weaknesses of these devices from a human factor perspective. Traditional network security focuses on two areas, "devices" and "procedures". Technology generally supports the devices area, with hardware and software devices that restrict access to the system, or to the system's data. Discussion of the devices available in this area is appropriate for this thesis. As these devices are all concerned with some aspect of the human user, human factors come into play. Procedures are methods that use organizational structures, such as compartmentalization of project teams, to control the dissemination of sensitive data. The goal of both areas is to limit or eliminate the potential for damage to the network.

B. POTENTIAL SYSTEM DAMAGE

There are several ways in which harm to or loss of data can occur in a network, with varying degrees of damage.

1. Destruction or contamination

Data can be removed from the system, or garbled so badly that it is rendered useless to the organization.

Depending on the data, this may or may not have serious consequences. For instance, the destruction of a list of attendees at last year's Christmas party may not be cause for alarm in the board room. On the other hand, employee pay records, or data that has been compiled at substantial cost to the organization may well be irreplaceable, and its destruction might be enough to cause the failure of the organization itself.

2. Theft or disclosure

In this instance, "theft" can actually mean "copied". This difference is important. When our society thinks of something being stolen, the normal conclusion is that some piece of property has been taken from its owner, and the owner no longer has it. However, data may be copied by an unauthorized person, yet the owner of the data still possesses it, and may not even know that it is no longer his alone. The mistaken assumption that the data is still exclusive knowledge may lead the organization to make poor decisions based on this false premise.

3. Modification

Programs that are essential to the health of the organization, or data that runs in these programs, must be highly protected. Changes in the programs or their data could easily lead to reduced organizational effectiveness. A possible scenario would involve a program for a petrochemical company that forecasts likely spots to drill for oil. If

either the code for developing the forecast, or the data leading to the drilling decision were changed, the company could spend enormous amounts of resources drilling in areas with no possibility of success, and ignoring areas of likely oil deposits.

4. Interruption or denial of service

Even if data is not actually destroyed or tampered with, damage to the organization can occur if required services are interrupted or delayed. These could include payroll processing, database updating, or financial transfers.

5. Resources used in eliminating intruders

If computer personnel are required to spend time isolating which user on a system is causing damage, this is time and resources that are not being spent in productive work. Finding and eliminating a disruptive user can take quite a bit of time, as an attempt is usually made to keep the search covert (Stoll, 1989).

6. Public embarrassment

Many organizations, such as banks, depend upon their reputation of security and trustworthiness for their business success. News of computer system infiltration could do irreparable harm in the loss of image, public confidence, or customer migration.

C. ACCESS CONTROLS

In all these cases, the degree of damage or amount of loss depends upon the criticality of the data accessed or of the function denied. For example, if the file containing the data for the last 10 years worth of annual reports is copied from the system, there is likely to be little effect. This is already public knowledge. However, if the data which will comprise the upcoming annual report is compromised, the organization could be severely affected.

This degree of criticality leads to various levels of protection of data. At the most basic level is encryption of the data itself. The technology for this method is well advanced, and definitely has a place in any secure network. However, encryption is generally invisible to the user, taking place at a level far below that with which the user interfaces. Encryption safeguards data from interpretation by making the transmitted data unintelligible, but it does not restrict access to the data. Access control measures, on the other hand, guard network resources by preventing unauthorized access. The two security methods complement one another and are more effective when combined. Encryption has little or no effect on the human factors involved in network security, and so will not be further discussed here.

When access control measures are used, human factors do come into play. Factors such as the ability to remember a password; the feeling a person gets when submitting to

fingerprint analysis, or the time it takes to key in ID numbers with a magnetic stripe card.

User authentication mechanisms can be divided into three categories:

- *What you know*, such as a password
- *What you possess*, such as a token
- *Something about you*, such as a fingerprint

1. Passwords

Passwords are probably the most common type of security device in use. A password is merely a sequence of letters, numbers, and/or symbols, that the system correlates with a unique user ID. The user inputs his ID and password into the system in order to gain access. The user ID is usually nothing more than the user's last name, but the corresponding password for that user ID is known only to the user, and must be input to the system, otherwise access is denied.

The theory here is that a user will keep his password secret. If it is known to no one else, then no one else should be able to access his account. In practice, however, users often pick passwords that are easily guessed. Spouse, children, or pets names are often used. While usually not that obvious, the vast majority of passwords hold personal significance for the user. They are thus are vulnerable to a "guessing" attack by an intruder with knowledge of the user's personal data, such as might be found in a personnel file, or through friendly association with the user.

While this method of "reasonable guessing" can usually discover one or two passwords in a large system, the more dangerous type of password attack is a "brute force" or "dictionary" attack. In this scenario, each word in a dictionary is tested as a possible password. With a computer program doing the testing and iteration, many thousands of words can be tested in a relatively short time, and with little effort from the human attacker.

There are several ways to increase the security of a password from both of these types of attack. The first action to take, though, is to restrict users from selecting passwords that reflect information contained in their personnel files. The examples mentioned earlier, such as family member names, can be extended to include street names, prior cities lived in, etc. This policy alone will virtually eliminate the ability to compromise a password through guesswork alone.

A good password has the following characteristics (Pfleeger, 1989). These characteristics are "good" from a purely security-oriented point of view. That is, they all contribute to the added security of a password, provided the password is used as intended. These characteristics do not take into account how the user could react to their imposition upon his password. Following the description of each characteristic is a comment on its human factors impact.

- It is composed of letters, digits, and other characters, so that the base alphabet for an exhaustive attack is large.

The number of possible combinations from a set of characters is x^y , where x is the number of legal characters, and y is the length of the password. If x , that is the base, is increased by the ability to use digits and symbols as well as letters, the base is significantly enlarged. From 26 possible letters, it goes to 26 letters, 10 digits, and at least 15 symbols such as @, #, and \$. This is a benefit to the security of the password if it falls under attack.

However, passwords composed of random characters are difficult for people to remember. A password such as "!r5*h+2" is unlikely to remain off paper very long. A user is likely to write such a password down, probably next to the terminal he uses the most. This practice is definitely not secure!

Another problem with a password such as this is that it is prone to keyboard error. The possibility of mis-keying is high, and this will cause extreme user frustration. It is also possible that the user may attempt to write some sort of script file for log-on to eliminate key-in errors. In that case anyone would be able to log-on using the script file, and the password would become moot.

- It is long, so that there are many possibilities for an exhaustive attack.

The length of a password directly affects the difficulty with which it can be guessed. This fact arises

from simple mathematics. Consider a password that is 5 characters long and may only consist of letters. There are 26^5 possible combinations available. By increasing the length of the password, the number of combinations rises exponentially.

This advantage is reduced considerably, however, by the introduction of human factors. The number of possible combinations consists mostly of random orderings of letters. As already discussed, people are unlikely to be able to remember a password such as "v#rpdmtqz", so they are unlikely to choose such a password.

People are more likely to choose short, easy to remember passwords, such as their initials, their wife's name, or the street on which they live (Haigh, 1984). If they are restricted from using passwords that are easily remembered, they will resort to writing them down. This is still not a good security practice.

- It is not a common word or name, so that a dictionary attack will fail.

A dictionary attack is the use of a computer program to try thousands of different passwords in an attempt to infiltrate the system. The password guesses come from a dictionary stored in computer memory, often the attacked computer's own memory.

If passwords are restricted from coming from the subset of words contained in common dictionaries, then a dictionary attack is likely to be unsuccessful. The problem

is that many common words appear in the dictionary, and these are likely to be ones that a user would choose. Forcing the user to forego words from the dictionary greatly limits his choices, and could cause some resentment.

- It is an unlikely password, not a characteristic related to the possessor, such as a spouse's name or a street address.

A great number of users choose passwords that are names of people close to them, or of other personal significance (Haigh, 1984). While easy to remember, (this is why they are chosen), such passwords are also easy for an intruder who knows the user to guess. This makes them less secure than they could be.

From the human standpoint, these type of passwords are very desirable. Using names of family members lends a feeling of comfort to the act of logging on, and makes the computer system less alien. Restricting these type of passwords from use is understandable from the security viewpoint, but disliked by the user.

- It is frequently changed, so that even in the event of someone's guessing it, the period of vulnerability is short.

The security advantages of this procedure are obvious. The less time a password is valid, the less time an intruder has to find it out. Users, however, do not like to change passwords. They grow comfortable with one, and it is easier to remember just one. In one case, a system required changing passwords monthly. One user changed his twice on each

changeover day, once to a new one, then immediately back to his old one (Haigh, 1984).

- It is not written down, so that it will not be found.

This is also obviously a good security practice. However, for the reasons already discussed, if a password is restricted from being within the group of commonly chosen, easily remembered passwords, it is quite likely to be written down.

2. Passphrases

One form of authentication that is similar to a password, but far more secure, is the passphrase. The passphrase is basically a longer version of the password. The argument concerning password length indicated that there are relatively few long passwords that people can remember easily. Examples of passphrases could be a line from a song or a poem. This would make a lengthy authenticator quite easy to remember. The important point to make about passphrases is that the user chooses his own. This makes it a more personal item, and more likely that it will be remembered without being written down.

Although the passphrase takes somewhat longer to enter into a computer system than the shorter password, the increased ability of people to remember a lengthy phrase as opposed to a lengthy random password is worth the small amount of added time.

3. Token

A token is the general name for an object that authenticates its possessor. For example, royalty used to be authenticated by a signet ring, and in many applications today people authenticate by ID cards. In order to be useful, a token must be unforgeable and unique. In practice, ID cards can be forged, but they are still used for authentication.

The "magnetic stripe" card is one form of token that can be used for network authentication. These cards are regular credit cards with certain information recorded in magnetic form on the back. The magnetic stripe is read by a sensing machine. Currently, this is often a machine that permits a customer to perform banking transactions day or night. These cards are not complete proof of authentication, as the card might be lost or stolen. A user of the card also has to enter an identifying word or number in order to use the card.

The strengths of a token are its two-tiered security, since an ID number and card must be used together, and its general acceptance by the public, through the large-scale Automated Teller Machine (ATM) implementation in use today.

The weaknesses of a token are that it must be carried with the user to access the system. The person may forget the token, or leave it in their other jacket. They may lose the token. They may feel the token is intrusive on their daily routine if it must be used often during the day.

4. Dial-back devices

The most vulnerable link in a network is a dial-up line. This is the first point of access in a network, and available for challenge by anyone with a modem and a telephone line. User authentication is difficult enough in a single computing system, but it becomes far more difficult when users can dial in from a telephone, literally anywhere in the world.

The Lineguard 3060 port protection device by Western Dataserve can protect up to 60 telecommunication ports, and has a built-in audit trail capability (Young, 1986). Dial-back devices such as this combine "what you know" with "what you possess". A user wishing to access a system through remote telephone lines is required to call from a designated phone number. The computer system being called will get from the user an ID number, and then hang up the phone. It will then search an internal database to determine if the user is authorized access. If so, it will call the user back at the designated phone number, and access can ensue.

Although this incurs a time delay for the user, it is unlikely to overshadow the convenience of remote access, most likely from home. The problem arises when the user needs or wants to access the system from another number not on the approved list. Once the user gets used to having this type of access, he may become indignant when he cannot.

5. Diskless Workstations

Diskless workstations are a relatively new phenomenon. They are similar to the standard mainframe terminal that many are familiar with, but have the added local processing power of a modern personal computer. As their name implies, though, they lack removable disk drives. This allows processing of sensitive information at the workstation, but eliminates the possibility of someone transferring that information from the workstation by way of removable media (magnetic disks).

This device has relatively little impact on the person using it. Projects that are relegated to these workstations must be able to be completed without transferring data by using disks, so there is little or no imposition caused to the user by the lack of disk drives.

D. BIOMETRIC ACCESS CONTROLS

Some devices are now available that can recognize physical characteristics of people, such as fingerprints, pronunciation, and patterns of the retina of the eyes. These devices provide highly reliable assurance of authenticity. Furthermore, fingerprints or pronunciation cannot be lost or stolen; they are not inconvenient to carry around, they do not have to be kept secret, and they are virtually impossible to forge.

There is, however, a learning curve for these biometric devices. Initial experiences tend to be negative, as the

false rejection rate is higher than the user might have experienced with authentication devices already discussed. As a user becomes more familiar with a biometric verifier, though, his false rejection rate decreases (Sandia, 1990).

1. Signature Verifier

Autosig Systems of Irving, Texas manufactures the Sign/On signature dynamics verifier. This device incorporates a user interface tablet which integrates into a host access system. The user signs his name on the tablet, and this signature is compared with a system copy of the signature. Variables such as pencil pressure and writing speed are considered. If the match is close enough, access is granted to the system. The false reject rate of such a device, for a trained user, is about 2%. (Sandia, 1990)

Problems relating to user acceptance of signature verification systems include a lengthy enrollment process. The user is required to sign his name at least 10 times to allow the system to create a composite "authorized signature". False rejects can become more common if the user attempts to sign-in rapidly, rather than slowly. This perception of delay retards user acceptance of the device.

2. Retinal Scanners

A retinal scanner is a device into which the user looks through a small aperture. The retina of the user's eye is scanned, and access is granted based on the pattern of blood vessels on the retina. These patterns have been shown

to be at least as unique as fingerprints, thus they have a good basis for a security access control. EyeDentify Inc., of Portland, Oregon manufactures a retinal scanner using the latest technological advances.

There is widespread public belief, however, that these devices contain laser beams, or are otherwise harmful to the eye (SCAT '90, 1989). Additionally, the device is somewhat invasive. The user must usually bend to the device, and then put his eye right on it. The only similar experience he might have had is an eye examination by a doctor. A large administrative effort is usually necessary to gain user acceptance among technically unsophisticated users.

3. Fingerprint Scanners

These devices require the placement of a finger on an optical pad. The fingerprint is then scanned for such features as print depth and pattern matching. Scans that correlate highly enough with the stored pattern in the system generate acceptance. Fingerprint scanners, such as those made by Identix, Inc., of Sunnyvale, California, average about 6 seconds for the process, but they have a false reject rate of approximately 10%. This is high for biometric devices, and causes much user frustration. In addition, according to a Drug Enforcement Agency report, when hands are cold, or the user is aged, the scanners tend to have higher false rejects (SCAT '90, 1989).

A fingerprint scanner is also subconsciously rejected by a user through association with criminal activity. Currently, the only other agencies that require fingerprints are of the crime enforcement variety. One hardly expects to be fingerprinted at work on a regular basis.

4. Voiceprint

Alpha Microsystems of Santa Ana, California manufactures a speech verification system called the Ver-A-Tel. This is a device utilizing technology whereby the sound of a spoken word or phrase is digitized, so that the computer system can store it, and compare it with later patterns of the same word or phrase. Verification takes only about five seconds, and the false reject rate is about five percent. This is generally acceptable for biometrics.

The enrollment process for a voiceprint system is tedious and lengthy, consisting of repeating the same word or phrase until the system grants a high recognition value to it. This method of authentication is well-accepted by users (SCAT '90, 1989). It requires the user to do nothing but speak, and gives him a feeling of "mastery" over the system. The system that responds to voice input also encourages the user to think of it as more than a machine.

5. Hand Geometry

A hand geometry verification device is similar to the fingerprint authenticator, but the whole hand is placed on the pad rather than a single finger. The added scannable surface

works to decrease the false reject rate to .2%. Such a device is manufactured by Recognition Systems Inc., of San Jose, California. This is a highly reliable security device, and well-accepted by the user (SCAT '90, 1989).

The process of putting the user's hand down on a pad is somewhat akin to shaking hands with a stranger, a commonly accepted practice in our culture. Processing time is quick, as little as three seconds. These two factors contribute to few problems in getting people to accept this type of device.

E. SUMMARY

This chapter described the types of damage that can occur to network data, and many of the authentication devices that can be used to eliminate or reduce the possibility of damage. In general, the devices discussed are all well suited to maintaining a secure system, but they vary greatly in user acceptability. Devices such as passwords must be monitored to ensure that certain ones are not used. Other devices, like tokens and retinal scanners have other attributes which discourage user compliance with security procedures. This chapter introduced the user acceptance or non-acceptance of these devices, later chapters will discuss methods for increasing user acceptance when the devices must be used.

IV. NETWORK SECURITY PROCEDURES

A. INTRODUCTION

Security managers and information systems managers must think of the availability of company resources as not in one fixed location, but removed by tremendous distances. Managers may not know where to install security systems, because they often do not know where all the terminals are. Organization-wide procedures must be established to provide standards for security throughout the system, since it is impossible for security staff to monitor each terminal or storage facility at all times.

This chapter discusses procedures, as distinct from devices, that can increase the security of a network. Procedures are organizational programs or methods that enhance the effectiveness of security devices already in place. They can also be security measures in and of themselves, without affecting any security devices.

For example, whenever an employee leaves an organization, an exit interview should be held. Aside from the managerial benefits of such an interview, it is an ideal time to collect security badges, keys, and any other security access devices from the employee. This time can also be used to initiate paperwork necessary to remove the user's passwords from the system. All concerned departments should be notified about an

employees's departure. This is an example of a security procedure.

B. SECURITY ENHANCING PROCEDURES

1. Password associated procedures

Research continues on even more sophisticated methods of authentication, but password mechanisms remain the dominant method of identifying computer system users. This is true for cost reasons as well as ease of use and user acceptance. The Internet worm of November, 1988, incorporated a password guessing routine (Oldehoeft, 1990). The guesses were comprised of: the null password, the username, the username appended to itself, the nickname, the last name of the user, and the last name spelled backwards. This guessing system typically broke 30% of the passwords in a system. In about 5% of cases, the default manufacturer password to a system was still active, often allowing system manager privileges (Stoll, 1989).

Iowa State University wrote a password guesser which was able to guess 15% of its systems passwords in 3 days (Oldehoeft, 1990). This was due to poor password choices, such as "uucp" for various Uucp networking logins. There are several procedures to focus the selection of passwords toward more secure choices than is normally the case.

a. Passphrases

The use of pass-phrases instead of passwords can greatly increase the difficulty of conducting a brute force attack. A four word phrase consisting of words from a 25,000 word dictionary yields 3.9×10^{17} combinations. One must be careful about enforcing too long of a pass-phrase length, however, lest users become irritated by keying errors. These phrases should also be checked by a guesser program for triviality, such as phrases like "Mary had a little lamb".

b. Password ageing

Password ageing is the enforcement of a maximum password lifetime. This is a procedure that can be used in conjunction with password selection procedures. It automatically gets users to change their passwords at some predetermined time interval. Although a good technique to decrease the vulnerability period of a password, it has possible side effects. If the lifetime is short, the technique may be counterproductive, resulting in user frustration at having to change passwords too often. If there is no warning mechanism to tell the user that passwords will soon expire, they may be caught unaware by the demand. This could result in a poor password choice.

To combat this last consequence, minimum lifetimes should be used to prevent users from changing passwords back to "easy" ones that they may prefer. For example, a user forced to change his password once a month might change it at

the appropriate time, then immediately change it back. This meets the system requirements for changing, but defeats the purpose of the procedure.

c. Password generation

A speaker on security methods often checked the inside of the hats of audience members prior to a lecture. He usually found pieces of paper with passwords written down, and used them in his lecture (Klopp, 1990).

It is far easier to maintain control over password selection in a system wherein passwords are machine generated and assigned to users, than one in which users may select their own passwords. However, as this story shows, there is a greater risk of password compromise in systems in which the user is not free to select his own password. In this instance, if the password is not one which the user can remember easily, he may write it down.

Password generation is a procedure in which a computer program is developed to create strings to be used as passwords. These strings are not genuine words such as may be found in a dictionary, rather they are strings of concatenated syllable components, joined so that they are easily pronounceable, and thus more memorable than a random sequence of letters.

One method of creating such passwords is to have an array of pronounceable fragments in the programs database,

with rules to govern their concatenation so that the resulting "word" is pronounceable.

d. Password monitor

This is a procedure whereby a computer is allowed to "grade" a user's choice for a password. This is accomplished by comparing the password with the database of a password guesser. A password guesser is a program that can conduct an exhaustive attack upon a system. Sources for an exhaustive attack on passwords are a large commercial dictionary, the reverse spelling of the words in the dictionary, a list of first names, last names, street names, and cities, all of the above with the first letter in capitals, valid license plate numbers, and the like. In a collection of 3289 passwords, 86% were found in one of the above sources of password guesses (Wood, 1990).

2. Auditing

Auditing of network activity is a procedure that can yield great benefits in security. Currently, much data about network activity is collected automatically by the network software, but it takes human intervention to act upon this data.

For example, the software may capture information associated with login attempts. It can store successful login and logout information, unsuccessful attempts, successful and unsuccessful password changes, and the programs or data areas accessed during a user session.

This information is useful only if reviewed and interpreted by security personnel. Programs can be developed to alert system operators to potential problems, but in the end, it takes a human being to evaluate and solve a security issue.

Auditing requires that controls generate sufficient evidence to show that they have been operating correctly. The evidence may take the form of logs, audit trails, reports, blinking lights, or other forms of obvious or hidden feedback. One of the most conspicuous examples involves password-based access control systems. These systems can generate voluminous logs showing when users logged-in, when they logged-out, the programs they ran, and the requests for access they submitted (whether approved or denied).

Without evidence that a control is operating properly, management cannot be confident that the control is in fact doing the job it is intended to do. Without such evidence, management is unable to make adjustments so that the control does its job better. Auditability is therefore an essential part of day-to-day management, not something just for auditors.

A more proactive view towards auditability involves what is called instrumentation. This refers to specific lights or other feedback that a control provides, such that if it fails or is being attacked, those responsible for the control are immediately notified. IBM has a system that

notifies the operator if someone is trying to guess passwords (Wood, 1990). The notification allows those responsible to take corrective or defensive actions promptly.

3. Concept of "Least privilege"

In the Department of Defense, this concept is identified as "need to know". It indicates that access to information, the ability to execute certain programs, and other system privileges should be restricted to those who can demonstrate a business or mission-related need. Modern system integrity theory applies this concept to data, programs, and users by allowing only certain programs to access certain data; integrity of the processes supported by programs is preserved by allowing only designated users to affect the processes.

A drawback of the "least privilege" concept is that if employees do not know what others are doing or how they are doing it, there is little opportunity for suggestions to cross organizational boundaries and improve operations. The concept can also make a workers' job boring or less productive than it might be. If users are unable to query the system for data they think could be related to their work, impatience and a feeling of frustration are probable.

4. Independence of control and subject

This procedure dictates that the person charged with design, implementation, and/or operation of a control should not be the same person who is to be controlled thereby. For

example, a programmer who is charged with writing a password authentication program for a certain system, should not subsequently become an authorized user of that same system. The potential for wrongdoing is great, since the programmer knows exactly how the authentication program works, and may in fact have built in a secret "entrance" to the program.

5. Separation of duties

This procedure prohibits organizational structures that involve conflicting loyalties or goals between or within departments. For example, having the Security function be a part of the Auditing Department would be unwise, because the Auditing department would then be unable to perform an unbiased review of Security.

This procedure can also be applied to individuals and project teams. Members of programming teams should not become authorized users on the system for which they are developing programs. This could lead to a possible compromise of the system at a later time. There is no known way to prevent the determined systems hacker from violating computer-based access controls if he is allowed to write programs (Browne, 1990).

6. Universal application

This is the consistent and all-embracing usage of a control measure across the spectrum of environments, computers, or people to be controlled. Exceptions to this rule weaken controls.

For example, top management may be exempt from a requirement to wear a badge when in the computer room. By virtue of this exemption, an interloper may enter the computer center, and having no badge, the staff may stay out of his way, regarding him as a new member of the top management team.

As another example, if only visitors are required to wear badges, a curious visitor who wanted to take a look around could easily masquerade as an employee simply by removing his badge. If badges must be worn by every person in a controlled area, the status of visitors and others in need of escorts or special treatment can easily be determined and consistently enforced.

7. Defensive depth

This is a procedure that increases security by providing multiple, overlapping controls. A physical analogy is a facility where a fence is used in conjunction with motion detectors and other physical access controls. If one of these controls is compromised or circumvented, the other controls provide a safety net to ensure that, in overall terms, a penetration is not successful.

Defensive depth is also found in the redundant use of a single control measure. This approach on a computer system would take the form of several layers of passwords being required on a network. For instance, a first password might be used to log into a local network node; a second password,

to gain access to a remote host; and a third, to get special privileges on the destination computer.

Defensive depth is a concept that implies controls placed in parallel rather than in series. Although both facilities in Figure 1 have two doors, the first configuration provides significantly less security than the second.

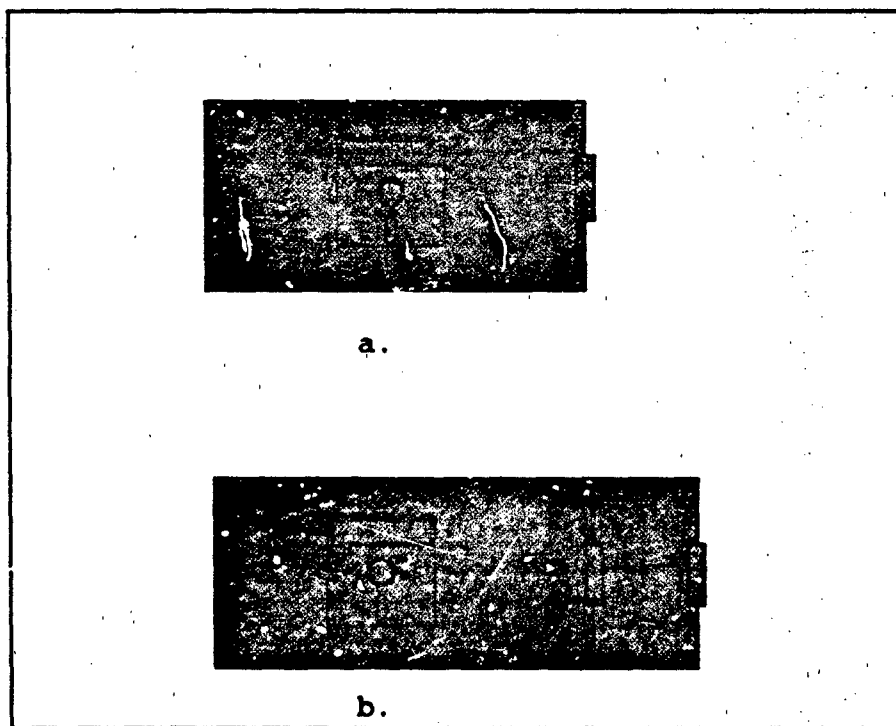


Figure 1. Defensive Depth

In the first, an intruder needs only get through one door. In the next configuration, though, it is required to pass through two doors to gain access to the computer room. The use of doors in the figure is merely illustrative, any security device could be used.

It is not necessary, nor is it desired, to limit access control to the periphery of a single large area. A space may be divided into smaller component areas. This permits limiting access for individuals to the areas which their job requires, and no others. Separate access controls may be applied to each of the areas that are components of the larger computing facility.

8. Least common mechanism

This principle seeks to minimize reliance on a central system component that may become unavailable. A physical analogy (Figure 2), shows that with a LAN built in the star configuration, failure of the central node will mean the network is unavailable to any node.

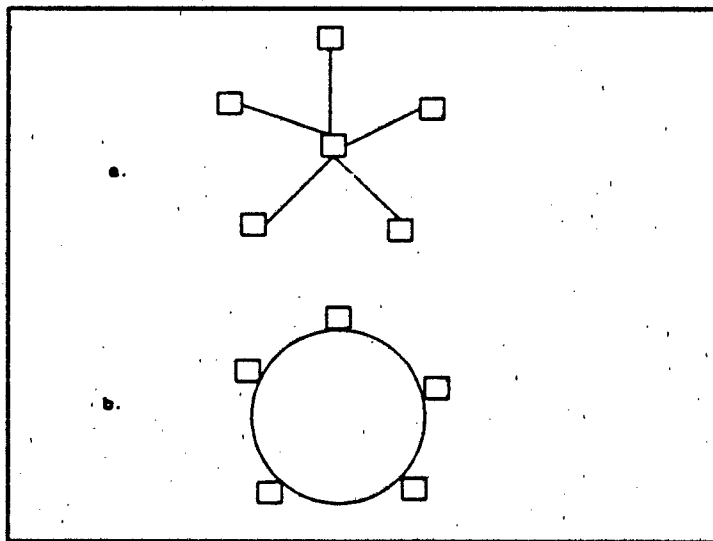


Figure 2. Least common mechanism

Failure of any one node on a LAN with a ring configuration, though, will not render the LAN unavailable, as traffic can be sent the other way around the ring.

The least common mechanism principle implies that the effectiveness of controls should not, to the greatest extent possible, depend on the proper operation of other controls. For example, if an organization uses automatically generated terminal passwords, but no user-IDs or system access passwords, it is implicitly relying on physical measures to control who may gain access to a computer. If this measure is compromised, no security exists. A more secure way to design this system would be to have two separate and independent procedures, one for controlling physical access, and one for controlling computer access.

9. Default to denial

When a control fails, which failure should be anticipated in any design, the control should deny access to users and other entities requesting service. For instance, the failure of an authentication device in a system should default the system to reject any attempts at user access, rather than allowing all attempts at access to be granted without authentication. This procedure prevents the devices from being disabled purposely in order to bypass them. Designers should appreciate that it is easier to turn a control off than to circumvent it, and plan accordingly.

10. Dial-up access

A good procedure to follow in the use of dial-up access lines is to route all dial-in users to a private branch exchange operator. This operator screens calls and asks identifying information of the caller. If the person is an authorized user, the operator switches the call onto one of the dial-up ports. No dial-up ports can be dialed directly. While this is better than many totally automated systems, it still depends upon human factors, which are subject to the quality of the person working the PBX at the time.

C. RISK ANALYSIS PROCEDURES

Risk analysis is part of the creation and improvement of any effective security system. There are several ways to conduct risk analysis, however, and management should be aware of the different methods' strengths and weaknesses. Typical risk analysis procedures follow, with discussion of their strong and weak areas.

1. Checklists

This is the traditional way to attempt control of risks. It is easy, and formalized. Its primary disadvantage is size. A comprehensive checklist for a moderately-sized information system can be several hundred pages (Shaw, 1988). Checklists may cover virtually all possible security problem areas, but they are rarely "system specific", and thus cannot cover every area for any particular system.

Neither do checklists provide any of the information necessary to make decisions. They are however, a good starting point for an analysis of a system, providing pointers to areas of potential trouble, and inducing in management a security mindset.

2. Quantitative risk evaluation

This procedure evaluates security in terms of cost of controls versus cost of information loss. It is the only practical means of evaluating the cost effectiveness of maintaining, improving, or reducing necessary security controls and procedures. A quantitative approach provides management with a means to evaluate the security proposal in a manner that they understand, which is dollars.

A problems with this approach, though, it that it tends to create the appearance of accuracy due to the use of concrete numbers. Action based on the assumption of good data is often dysfunctional to the organization. Management must understand that these numbers are only as good as the estimates of the value of information.

3. Scenario-based method

This procedure is based on a scenario-oriented analysis of possible risk factors. Scenarios are developed of potential damaging incidents, such as loss of CPU availability, and the cost associated with the loss is estimated. This type of analysis is normally carried out by both the systems' users and risk management experts. Its

chief problem is that it contains forms and questions which require extensive investigations and the use of experts. These investigations may be impossible for an organization to conduct, or the experts needed may not be available. A positive effect of this procedure is that it gets the users involved and emphasizes the importance of risk control.

4. Qualitative risk analysis

This method assimilates the qualitative evaluations of the security manager in an attempt to come to a general conclusion about the systems' security. Its primary usefulness is in identifying problem areas. As with the scenario-based method, it requires an expert evaluation, which may not be available. It is not well-suited for developing solutions to the problem areas identified.

D. SUMMARY

Network security procedures can enhance the effectiveness of security devices, or stand alone as security elements in and of themselves. Standard organizational security procedures can greatly improve the security of an information network.

Procedures such as password ageing, auditing, and separation of duties can all decrease the security risks associated with a system. Procedures, though, are as dependant as devices upon the proper attitude and actions of the human operator. Auditing, for example, is merely the

gathering of useless information, if a person does not take the time to review and act on the information gathered. If a defensive depth procedure is seen as unnecessary, or too time-consuming, it may be circumvented. Human factors are the final arbiter of a procedure's effectiveness.

Risk analysis of networks involves one or more procedures to determine the need for controls, or the effectiveness of current controls. The usefulness of these procedures also are dependent upon the quality of the people involved, and the actions taken after the analysis is complete.

The security procedures reviewed in this chapter show how organizational actions can have a positive effect on the security of a network. It also shows that this positive effect can be undermined if human factors are ignored or undervalued. The next chapters discuss various methods of increasing user motivation to follow correctly the security procedures in place.

V. FACTORS AFFECTING SECURITY MOTIVATION

A. INTRODUCTION

Security controls are a vital part of any information network. They are needed to protect data and programs from unauthorized modifications or disclosure. The controls can be as simple as a password authentication system, or as complex as multi-level, multi-token access control. Any method of control, however, affects the user. If controls are not acceptable to users, or to others who are affected by such controls, ways will invariably be found to overcome or ignore them.

Basically, people resent controls. Whether it is safety belts in an automobile, or time limits on CPU usage, people dislike being subjected to mechanical restraints. Left to their own devices, people often circumvent or disable control mechanisms. Control mechanisms are also useless unless people pay attention to them.

A discussion of methods to motivate users toward security consciousness and security-oriented behavior must first identify the positive and negative human factors that affect security. Chapter III discussed how certain security devices inherently imply particular attitudes toward these human factors. Chapter IV did the same for security procedures. This chapter further defines and explains these factors, in

order to allow later development of methods to promote the positive factors and diminish the negative ones. It also introduces a chart depicting the relative importance of the presence or absence of specific human factors as applied to specific network security controls.

B. DEMOTIVATING FACTORS

1. Security control forced upon user

The interpersonal communications needed to gain user support for security controls are often forgotten in the effort to create a security control system, or patch up an inadequate existing system. Management often treats the involved people as though they are just another part of the system, without feelings, concerns, and other uniquely human attributes requiring special consideration.

An example of this factor in action is when a user password is chosen by the system administrator, with no input or involvement from the user himself. This type of policy may well be the most efficient security measure, enabling the administrator to easily control passwords and limit access. Excluding the user from the process, though, can negate any benefits.

Time must be invested to gain acceptance from the people involved, to train those same people, and obtain their cooperation and support. To do otherwise, management invites sabotage, work slowdowns, and other rebellious responses.

2. Control takes a long time to perform

Consideration of the performance impact on both involved humans and involved computers is an important element of attaining the acceptance of subjects of security control. If there is an adverse performance impact, and users are given no dispensation for the changed circumstance, acceptance will be most difficult to obtain.

For example, if data entry personnel get paid based on the number of transactions they enter, and if management introduces a control that slows their data entry work, the staff would be likely to object, unless there was a corresponding adjustment in the pay rate.

Security procedures in depth also tend to demotivate users, particularly if the ratio of time spent on the controls relative to time spent in work is high. For example, a user who must pass through multiple security controls each time he enters a secure application, may spend more time passing through the controls than doing the work. This user will be inclined to work less on the application than may be necessary, perhaps falsifying records indicating that data has been checked or updated.

3. Control interferes with user's routine

Security controls that interrupt a person's daily work routine, or cause that routine to be altered, will be met with resistance. Types of controls that could interfere with

normal work routines are default to denial systems, overuse of token systems, and certain dial-back mechanisms.

Default to denial schemes are controls that, when disabled or absent, result in denial of resources to the requesting user. This can annoy users if, for instance, a malfunctioning security system resorts to tersely denying entry rather than explaining the reason to the user. A simple message stating that the control is inoperative, thus access cannot be granted, would allow the user to seek help from the system administrator rather than be frustrated by a cryptic denial.

Excessive use of tokens in a security control system can also greatly irritate and discourage users. At a well-known computer manufacturer's facility in Italy, a magnetic card-based physical access control system was installed on nearly every door in the data center. Every time employees went into the hall, the washroom, the lunchroom, or other areas, they were forced to insert their card into a wall reader. The effort and inconvenience this procedure caused resulted in the workers going on strike. Such a reaction may have been avoided if the use of the cards had been reserved for true security purposes, rather than as a control on every door. (Wood, 1990)

Dial-back systems can interfere with work habits well. In particular, systems that allow for only one authorized number per user. In this case, a user is

restricted physically to one location in order to use a computer phone line. If work or convenience compels the user to be at a different phone number than the one held by the system, then the user's motivation to work will decline.

4. Control is invasive

The previous example of the Italian firm that required card insertion at every door in the workplace was also perceived by the employees as an unwarranted invasion of their privacy (Wood, 1990). Employees are justifiably bothered by what seems to be management's attempt to track their every move.

Another aspect of security control that does not sit well with many employees, particularly professionals, is the fact that an organization's information does not belong to the employee, even though the employee may have produced it. Employees are reluctant to treat an organization's information holdings as assets that should be protected. This attitude is reflected in incidents of reported employee indifference to the damage created by some computer viruses, and by the apparent resurgence of business espionage (Wood, 1990).

This unwillingness to protect an organization's computerized information assets seems to be heightened by an idea propounded by some microcomputer networking enthusiasts. These people contend that everyone who works for an organization should have unlimited access to all the information that the organization possesses. This practice is

supposed to improve job performance. However, it is more likely to lead to increased friction between individual employees, as well as between some employees and the organization's management. (Menkus, 1990)

Americans typically contend that imposing any form of control over the way in which they spend their working time is repressive, and an invasion of their personal privacy (Shain, 1989). They may feel that such control interferes with their prerogatives as self-motivating professionals.

5. Management not committed to controls

No security system, no matter how technically efficient, can succeed without the support of the management in the organization. If the users of a network see that management is not concerned with the security aspects of the information system, neither will they be.

Security-oriented behavior needs to be recognized as an important part job performance. The lack of this aspect of the job in most organizations performance evaluations contributes to the notion that management does not view the area of security as important.

The principle of universal application, as discussed earlier, also bears on the question of management commitment to security. If management exempts itself from controls to which other employees must submit, then the organization is sending the message that security is only a minor issue, and

not important enough to require the support of every member of the organization.

C. MOTIVATING FACTORS

1. Involvement in the control process

In any security system, it is important to involve the subjects of the controls in the process of developing and implementing those controls. This does not mean that controls should be subject to user approval prior to implementation, only that involvement in the process is vital to user acceptance.

This involvement should start upon the hiring of new employees, with an interview in which organizational security policies are defined, and the reasons behind the policies explained. It must carry on to the implementation of security controls, as in the use of a password assistance program, which can offer choices of computer-generated passwords. This way the security manager maintains control over the choice of passwords, yet the user is able to participate in the process and feel a sense of freedom of choice.

When changes are planned for a system, the changes must be discussed with the users, or the users must at least be informed that the changes are coming, and their purpose in the system. Changes to a system that are made without preparing the users are resisted (Leemah, 1986).

User involvement can also be achieved through training and education. The sense of interpersonal relationship is significantly reduced when dealing with a computer. There is a feeling that ethics are for people, not machines. The more directly personal a relationship is, the more acute our ethical sensitivity becomes. We seldom have the same emotional reaction to a computer that asks us to key in an appropriate response as to a person who asks us a question.

If, through education, users can meet with security personnel, see who they are, and learn what their specific responsibilities are, ethical standards the users are familiar with may seem applicable to the network environment, and thus be effectively harnessed for network security.

2. Personal responsibility for controls

Legally, employees commonly are held to share in asset protection responsibility. This general asset protection obligation has been supported in the United States in numerous court cases and labor arbitration hearings. (Menkus, 1990)

In most organizations this obligation to protect critical information assets is not established as a standard condition of employment. Thus, for example, where that responsibility has not been delineated in a structured fashion, an organization's professional and technical employees may feel they are free to share unlimited amounts of sensitive, and even proprietary information with others in their particular profession.

Responsibility must be placed squarely on the user's shoulders through explicit instruction and written contract. Informing a user that his password identifies any actions on the network as his own, unauthorized actions included, will serve to promote proper safeguarding of passwords. People will be less likely to share or write down their passwords if they know that they will be held responsible for all network sessions using that password.

Responsibility for security is a rule that must be highly publicized and known to be strictly enforced. Swift and appropriate punishment for security breaches will motivate users to be more security conscious. If a person knows that failing to follow proper procedure may result in the loss of clearance or even his job, compliance will increase. An atmosphere in which punishment is rare or insufficient will do little to promote security-minded behavior.

3. Reward users for good security practices

The counterpart to swift and just punishment for security infractions is a system for rewarding those who show good security practices. Already mentioned was the inclusion of security behavior in the performance evaluation, but other types of reward systems can also be effective.

Normally monotonous tasks, such as checking audit logs, can be seen differently if an auditor knows that he will be rewarded for finding discrepancies. Just as punishment increases people's desire to avoid security infractions,

rewards provide an added incentive to maintain good security practices and detect poor ones.

4. Easy, fast, and accurate controls

This factor acts as the opposite to the demotivating factor of difficult, complex, and error-prone controls. If a control is easy to use, people will naturally be more likely to use it. If it does not slow down their normal working pace, they will be less likely to avoid it. If it is accurate in its execution, it will avoid promoting frustration in the user. All these aspects of this factor are desirable, and increase the probability that a user will employ security controls.

5. Users are comfortable with controls

This factor alludes to the mention in Chapter 3 of certain controls with which users are instinctively comfortable. Specifically, controls like signature verification and Personal Identification Numbers.

Using a signature for authentication is an action that has been around in our society for hundreds of years; the application of that act to computer networks is an easy transition. Personal Identification Numbers, though not as historically ingrained, have enjoyed widespread acceptance for many years in the form of ATM authentication. Again, the transition to information systems use is an easy one.

Incorporating into controls ideas and actions that are familiar to users is a way to reduce the natural resistance to

change that always exists, and take advantage of secure methods of control toward which users are already favorably disposed.

6. Management support of security controls

This factor has been mentioned several times already in various contexts. It is an integral part of any successful security system, thus it has bearing on many different facets of the system. Without management support, the organization as a whole will neglect security as an effort not worth taking. Visible, constant, and unquestioned support of security goals must be management's contribution to the security of a network information system. Such support will act to create similar attitudes throughout the organization, and foster a sense of "corporate awareness" of security issues. Once this attitude becomes firmly ingrained in the organization, it will become an institutionalized attitude, extremely difficult to change, and the source of peer pressure in support of security goals.

D. HUMAN FACTORS IN SPECIFIC SECURITY CONTROLS

Developing a methodology for incorporating human factors into security controls requires first that each factor's effect on the different controls is quantified. To implement a control, some idea of the relative impact that a particular human factor has on that control is necessary. The following

is an attempt to quantify the relative effect of the human factors previously discussed.

Every security control creates a feeling in each individual user, either of acceptance or rejection, merely from the method of control itself. For instance, voice recognition systems give power to the user over the machine; his spoken "command" results in the machine's compliance. A dial-back system, however, requires the user to conform to the system's desires; he must be at the phone number the machine recognizes. These inherent characteristics of the security control are impossible to change, but an enlightened security administrator can bring to the control the human factors that aid in user acceptance, and try to remove from the control those factors that block acceptance.

E. SECURITY OPTIMIZATION

Figure 1 is a chart showing the relative importance of specific human factors as applied to specific security controls. The values at the intersection of a factor and a control indicate how strong the interaction is between a specific factor and a specific control. A "+" sign denotes a favorable interaction, a "-" sign, an unfavorable interaction. The values range from +5 to -5, with a "---" indicating no interaction.

To interpret the chart, use the intersection of Passwords with Management Support, the value is +2. This shows that a

		Control-related					Organization-related					
		Comfortable Controls	Lengthy Control	Interfering Control	Invasive Control	Fast Accurate Controls	User Involvement	Personal Responsibility	Users Rewarded	No Management Commitment	User Forced	Management Support
Devices	Passwords	+3	-3	-1	0	+3	+2	+3	+1	-2	-2	+2
	Passphrases	+3	-2	-1	-1	+2	+2	+3	+1	-2	-3	+3
	Password Ageing	+2	--	-1	-1	+2	+2	+4	+1	-1	-1	+1
	Auto Generation	+1	--	--	0	+2	+3	+2	+1	0	-2	+1
	Password Monitor	0	--	-1	-1	+2	+1	+3	+1	-1	-1	+1
	Dial-back	+1	-2	-3	-1	+3	+3	+4	0	-1	-2	+2
Biometrics	Diskless Workstation	+1	--	-2	-1	--	+2	+2	+2	-2	-2	+2
	Signature Verification	+3	-2	-1	0	+2	+4	+3	+2	-1	-1	+4
	Retina Scan	0	-2	-2	-3	+2	+2	+5	+1	-2	-2	+2
	Fingerprint Scan	+1	-1	-1	-2	+3	+3	+5	+2	-1	-1	+4
	Voiceprint	+3	-1	-1	0	+5	+4	+4	+3	-1	0	+5
	Hand Scan	+3	-1	-1	-1	+5	+4	+5	+3	-1	0	+5
Procedures	Control/Subject Independence	0	--	-2	-1	--	+1	+3	0	-2	-2	+1
	Separation of Duties	0	--	-2	-1	--	+1	+2	0	-1	0	+1
	Universal Application	+3	-1	-1	0	+4	+3	+3	+1	-2	0	+4
	Defensive Depth	+2	-3	-2	0	+4	+3	+4	+1	-2	-1	+2
	Least Common Mechanism	+2	-1	-1	0	+3	+2	+3	0	-2	0	+2
	Default to Denial	+2	-1	-1	0	+2	+2	+5	0	--	-1	+2
	Auditing	0	-3	--	-1	+4	+2	+3	+2	-3	-3	+2
	Least Privilege	0	--	-1	-1	--	+1	+3	+1	-2	-2	+1

Figure 1. Security Optimization Grid

if a password system is implemented with the support of management, and if the support is conveyed to users, the system will be accepted and supported by those users. A value greater than +2 would indicate a higher degree of acceptance and utilization. A value less than zero would indicate a poor degree of acceptance and possible attempts to bypass the control.

An example of the unfavorable situation is the value at the intersection of Passwords and Lengthy Control, -3. This shows that if the password is too long, the effect on the user will be negative, and the magnitude of the value indicates that this may have relatively serious consequences on security. The user will be likely to write down the password, or even create a "logon script" to bypass entering the password directly.

1. Using the optimization grid

When a manager can interpret the grid, he can then use it as intended, to optimize the security situation for which he is responsible. There are 2 ways to use the grid for security optimization.

The first way is used if the controls of the organization are a given. In this case, the manager can enter the grid on the row containing the control used in the organization, then go across the row to find the highest value in that row. The manager should then attempt to implement the

human factor at the top of that column. This will optimize the degree of security possible for the given control.

The second way may be used if the human factors in the organization are more set than the controls. If the organizational environment is such that the security manager cannot affect them, then he can enter the grid at the top, at the factor that exists in the organization. He can then go down the column until reaching the highest value in the column. The security control in that row will be the one that optimizes security, given the human factors in place.

It is likely that in any organization, neither the controls nor the human factors are set in stone. In this case, the security manager can pick and choose the optimum combinations for increased security. In any case, though, the manager must first determine what factors in the organization he can influence, and how great his influence can be.

This chart can be useful in maximizing user acceptance of and compliance with network security controls. It can be a guideline when implementing controls, or when improving existing controls. It is important to realize, though, that the values are subjective, and may need to be adjusted for particular organizational cultures or work environments.

2. Grid divisions

The security optimization grid can roughly be divided into 6 areas. Among the controls, 3 divisions are relevant. Devices, procedures, and biometrics. Biometrics are properly

a special case of devices, but deserve added analysis. Among the human factors, 2 groups appear, those that are control-related, and those that are organization-related. For example, forcing users to accept a password, with no input in the process, is a function of organizational procedure, not a factor of the password itself.

D. SUMMARY

This chapter discussed in detail some human factors that directly impact the security posture of a network information system. To ignore these factors in creating or upgrading security systems is to invite the users to ignore and circumvent the controls. The users are the heart of any information system, and a lack of regard for factors affecting them is not good management. It also introduced a quantitative tool to assist in the development and adjustment of security controls, in order to optimize security. A discussion of methods of security control that take best advantage of the human factors discussed, is the subject of the next chapter.

VI. ENHANCING SECURITY CONTROLS: A HUMAN FACTORS PERSPECTIVE

A. INTRODUCTION

Personnel from within an organization present the greatest threat to its security system, yet they can also be its greatest security control (Parker, 1990). Many employees understand their organization's system and work with its data on a daily basis. Their relative ease of access to data gives them the best opportunity to abuse or manipulate it. Yet, this daily interaction also gives them the best perspective from which to detect data errors or security breaches. The strength of a security program is based largely on security awareness and compliance by employees.

This is the premise of this thesis, and this chapter combines the previous discussions of human factors and security controls into practical methods to achieve network security.

Many security directors step into a job and inherit the existing system, along with all its faults. Unfortunately, there are often more pressing demands on the director's time than to undertake a major change in the security system. It appears that the old adage, "if it works, let it alone", is accepted where security is concerned. Unfortunately, the fact

that there have been no security breaches detected does not indicate that the security system works.

There are two primary defenses against insider crime. The first is to reduce the opportunity to misbehave undetected. The second is to counter the rationalizations people use to "justify" their misbehavior. The way to achieve the first goal is through improvements in the physical security system and organizational security procedures. To achieve the second goal, a change in the ethical environment of the organization is needed. This change can be realized through an ethics education program, user involvement in the system, and user training in the standards and procedures expected.

There are several prerequisites to implementing these defenses. An evaluation of the current security system is necessary, to identify its weak areas. Support for an improved system must be gathered, both from management and from the user community. The actual implementation of security improvements must be made, and methods for maintaining the improved state of security must be put in place.

B. EVALUATING THE CURRENT SYSTEM

An evaluation of the current state of security in the existing network is a necessary step in the process of increasing security and building support for the security system. The first phase of an evaluation should be to

determine the existing controls. Often the system has been in place so long that the controls in place are not adequately inventoried.

The second phase is to determine if the controls are adequate for the information being protected. This phase should be completed with one of the risk analysis methodologies discussed in chapter IV.

The third phase is then to use a tool such as the Security Optimization Grid to plan to optimize the controls that are to remain in place, as well as those that are to be added.

As an example, assume that a security manager enters an organization after the first two phases have already been completed. The existing controls of a password system, a dial-back system, and a universal application strategy are considered adequate. Management has determined, however, that a retina scan device is needed to protect a particularly sensitive area that has been added since the current security system was developed.

The question for the new security manager is; how might the existing controls be improved, and how can the new control be introduced so that it achieves maximum effectiveness. An evaluation of the situation using the security grid will yield the answers.

First, look at the controls that are to remain in place. A password system, according to the grid, yields greatest benefits when it is fast and accurate, and personal

responsibility for the password is maintained. A dial-back system also works the best when personal responsibility is maintained. User involvement is an important human factor, but the system is already in place, so the time for user involvement in the process is past optimum. A strategy of universal application of controls has its best performance under conditions of management support. The controls already in place can benefit from the implementation of these human factors.

As for the control yet to be implemented, the retina scan, the security grid shows that speed and accuracy, personal responsibility, and management support are most important to its success. The Security Optimization Grid is useful in assisting security personnel in choosing the human factors that maximize the benefits of particular controls. It can also aid in selecting those controls that are most effective given a particular human factors environment.

C. BUILDING SUPPORT FOR IMPROVEMENT

1. Management support

Information is likely one of the critical assets an organization has, and is probably very poorly perceived in that regard. Most people do not consider data an asset, and the vast majority of laws in existence today do not recognize data as an asset (Silverman, 1990).

But computer criminals have done a service for security managers. They have taken a subject about which most people know little, and brought it to the pages of Newsweek and Time. Security officers can use highly publicized incidents to help convey the seriousness of the situation to top management. Support may thus be gained for security improvements; support that might otherwise be focused on more immediate, short-term aspects of the organization.

With this in mind, a key role of today's security officer is to educate management. Senior managers tend to know little about security and less about computers. They frequently assume that computer security is a technical problem calling for technical solutions. Security officers must take an active part in resisting this perception, and educate upper management to the real nature of security and control.

This education has as one of its goals, a statement detailing management's policy on network security. Such a statement is vital so that users will know what the policy is, and exactly where management stands on security issues. The statement of data security policy should address broad security issues and clearly outline organizational policy. Such a policy should, at the least, state that:

- Data is a valuable asset that needs to be protected.
- Protection of data assets is the responsibility of all employees, not just data processing personnel.
- Only authorized individuals may access the company's computer system.

- Employees are responsible for reporting suspected misuse, fraud, embezzlement, or disclosure of organizational data or resources.

Security policies need to be clear to all users. Management must determine, before a violation occurs, whether the organization is willing to prosecute security violators. Making it clear that abusers of the system will pay the consequences of their actions can serve as a significant deterrent to computer crime. One of the greatest reasons for not committing a crime is fear of getting caught. Management can create a strong disincentive if they make it clear that abusers will be punished.

The security policy document is the foundation for a good security plan. The policy sets the tone for security attitudes, and the security plan provides for the practical implementations of that attitude.

a. Security plan

To overcome management's lack of appreciation for the importance of information security activities, it is well advised to develop a convincing information security plan. The preparation of a plan provides an opportunity to talk with key high level managers responsible for information security. Additionally, it is through the writing and revision of information security plans that conversations about why the information security function exists or should exist can evolve.

It is through a plan that conversations about who is responsible for information security, how the function should be centralized or decentralized, and the like, can be generated. It is through a plan that management commitment, and buy-in from various other groups, can be obtained.

The security function cannot wait until circumstances force changes. Instead, it must generate a sense of urgency about security, and communicate this to others. It can use technical and business knowledge of the system to do this. An effective way of communicating what must be done, and its urgency, is through an implementation plan for new and more effective systems control measures.

Formulation of a security plan involves 6 phases. (Zviran, 1990).

- Identify IS assets
- Assess threats and risks
- Analyze vulnerabilities
- Evaluate existing countermeasures
- Evaluate needed security level
- Formulate a security plan based on identified needs

These are general guidelines for a security plan, but one item that should specifically be included in the plan are provisions for a standards manual.

Information about computer operations and computer security should be included in the organization's manuals of standards. Existing manuals are available that can be used as

models for creating a new manual, or evaluating existing standards.¹

Each employee should receive a manual, and sign a statement acknowledging its receipt and agreeing to abide by its provisions. Manuals should describe expected security procedures and precautions.

Manuals are important because they establish a common understanding. A manual sets forth in black and white what is allowed, what is expected, and what is against the rules. With established organizational standards, rules can be applied uniformly to everyone. Well-prepared manuals address infractions of policy by prescribing appropriate types and levels of disciplinary actions.

It is important to have a security plan. Without a plan, the information security function cannot respond rapidly to changing circumstances, because its priorities are unclear. Without an appropriate plan, the communications gap between the technical community and management is likely to widen. A plan ensures that both groups work together synergistically.

However good the plan, though, if top management is not behind it, through its policy statement and its actions, the plan will be ineffective. Security professionals must be

¹ An excellent manual to use as a model is available from the City of New York, System Security Standards for Electronic Data Processing, Sales Manager, Citybooks, City Records Office, 2213 Municipal Building, New York, NY 10007

able to "sell" their plan to the people in charge of the organization.

b. Selling the plan

To "sell" a security program to management requires:

- Establishing a need for it.
- Providing a means to fulfill that need.
- Ensuring that the benefits of meeting the need outweigh the costs of not doing so.
- Making sure that people understand the need and the benefits of the program.

One time-tested way to ensure management sees the need to address an issue is to frame it in dollars and cents. However, it is impossible to compute the numerical, dollar cost of not having security. It is also impossible to compute the cost of not having disaster recovery planning. But it becomes crystal clear what those costs are if your security is penetrated, or if you suffer a disaster, and serve as the lead story on page 1 of ComputerWorld. Until you suffer a loss, though, there is no way to cost-justify security on a purely monetary basis. This is the message that must be conveyed to management.

Except for security professionals, no one understands all the ramifications of the network security problem. The use of examples from other companies about the hazards of neglecting security can be useful. Trade magazines often have stories of security breaches, although usually these are anonymously reported. A somewhat dramatic, though

potentially effective technique might be to have management view the film "War Games", to get their attention.

Another way to get across the need for security is to set up a "tiger team" from people within the organization. This team can attempt unauthorized entry into the system. If knowledgeable computer personnel are chosen, the odds are good that you will have quite a scenario with which to brief management.

The bottom line is, use whatever means are necessary to get those in charge to realize the importance of security. Then the need for security will be established. The means to fulfill the need are contained in the security plan, therefore, management now needs to be sold on the benefits of the plan.

Recommendations that increase revenue, without incurring additional cost or generating controversy, are sure to get priority. Similarly, recommendations that increase the output of products and/or services, without increasing costs, are always winners. An example is a plan for improving the rate of data input through error reduction rather than adding operators. Error reduction increases security by making systems more resistant to unanticipated actions.

Recommendations for reducing operating costs are also attractive. Reducing costs by decreasing staffing requirements is often appealing. For example, reduce the

number of contract security guards by increasing the number of surveillance cameras.

Convey to management that the use of an information classification system can also produce savings because, while it identifies valuable information that requires protection, it also identifies less important information that may be unnecessarily protected by costly security measures.

Computer security is not cheap. Senior management must be sold on the program in order to release the dollars. Do not lose sight of the fact that senior management is your ultimate buyer. But they have to understand what they are doing before they spend the money.

Security managers should avoid excessive technical detail in explaining a program. Security is a business problem, not a technical problem. It can, and should, be explained in business terms, and it can be presented for business analysis using traditional business principles of efficiency, overhead reduction, etc.

Leave all your technical jargon back at your desk when you talk about elements of security. Talk about transfer rate in terms of pages of a report vice baud rate or megahertz. Talk about error reduction in terms of increased efficiency of order entry and processing. These are the arguments that will convey to management the need for, and the understanding of, security in the organization.

2. User Support

a. Ethics program

Despite all the good an information ethics education can do, it would have virtually no effect on a true criminal (Parker, 1990). If a person is going to commit fraud, embezzlement, or extortion using information systems, his method may be very different from the non-automated variety of criminal, but his ethical values are likely to be very similar. His response to an information ethics program would probably be no greater or less than to any other kind of ethics program.

What is of more concern is the far larger population of well-intentioned and usually well-behaved people. Their ethical standards are foggy because of the unique information-related ambiguities and conflicts already discussed. This is where a well-structured and executed ethics program can bear significant fruit.

Any successful program of information ethics must take the reality of human nature into account. People will not be models of restraint in communication with no more guidance than a statement of policy and an occasional awareness meeting. Expecting confidentiality to be maintained with no ethics program in place is unrealistic.

The first principle of what works and what does not in an information ethics program is: Make it specific and target it to the audience. Spell out in specific detail what

information is proprietary, the reasons it is proprietary, and how it is to be protected. Employees who commit computer crimes are frequently first offenders who don't think of themselves as criminals. When asked about their activities, they often fabricate legitimate-sounding reasons to justify their actions (Zimmerman, 1990).

An important factor in deterring such crimes is to make it abundantly clear that such activity is wrong and illegal. This can be done by labeling everything related to EDP activities with gentle reminders. All equipment, documentation, forms, and program headings should contain a label that states ownership and legal uses.

An ethics program must be accompanied by local recognition and commitment. Unless a user's own management and peers actively adopt and support the program, he will regard information ethics as just another effort from corporate staff. What is needed is a combination of generic material and specific local material with which the user can identify, and to which he can make a personal commitment.

One way to bring the program home to the user is to identify the people responsible for local aspects of network security. That part of the emotional reinforcement one's conscience receives in a personal relationship is missing in an electronic connection. If the organization cannot make its information system more personal, it can at least clearly identify the people behind the system.

What makes information ethics a reality in an organization is the force of peer pressure and attention from local management. An attitude of security is best transmitted by local managers who themselves have "bought into" the program.

The premise that peer influence plays a primary role in creating an ethical environment is the central tenet of an Air Force security plan called "Keystone" (Prause, 1985). There are 6 steps in the plan. They work together to create, and foster, an environment where security is the norm. People being human, they then attempt to emulate the normative behavior of the group, resulting in a secure environment.

The steps of the Keystone plan are:

- Proclaim the Guiding Philosophy
- Reach an Informed Consensus
- Publish the Rules
- Know who uses the Computer
- Investigate Every Deviation
- Establish Due Process Discipline

In the ambiguous realm of ethics, if a certain level of behavior is desired, specific and detailed direction is required.

b. System involvement

Enlisting the active participation of employees in planning, designing, and maintaining a security system is probably the single most constructive tactic a security officer can adopt. The perception that security is an us-versus-them idea must be avoided. A positive attitude is more

likely to result when employees can participate in security system decision-making rather than having to accept rules and regulations imposed on them by authoritarian mandate.

Americans have a deep-rooted inclination toward complete freedom of choice. Their first reactions to controls, restrictions, and procedures are resentment and defiance. This posture is aggravated when rules seem arbitrary or capricious. To avoid negative feelings, information should be provided about the reasons for security actions. In a well-designed security system, every control exists for a reason. The justification for each security measure can and should be provided to employees. If a control cannot be justified, it should not be imposed.

One way to involve people is to give them a stake in the success of the system. People do what they are rewarded for doing. One of the strongest motivators for an employee is the regular performance evaluation. If employees are rewarded on their evaluations for good security practices, the program will benefit. Security-related performance should be included in the evaluation criteria for employees; its presence on the evaluation form will reinforce the perception that management is serious about security.

A more direct method of involvement is to solicit user's input when establishing a control. At General Dynamics, installing a dial-back system was made smoother through management involvement. "Getting them involved and

informed early was critical to our success," said W. E. Tucker, the project manager (Leemah, 1986).

Before GD's dial-in system was even up, users were informed that a change was on the way. By notifying them early, Tucker believes he minimized the resistance to change. An explanation of the system and its purpose removed any resistance (Leemah, 1986).

General Dynamics also incorporates security into its organizational culture by including it in its motto: Security in my job means job security and I take it seriously (Leemah, 1986).

Status symbols at General Dynamics are "Official Computer Crime Fighter" sweatshirts and windbreakers, which are awarded to employees who display a high level of security awareness (Leemah, 1986). Involvement of the user into as many aspects of security as possible is the best way to encourage a secure networking system.

c. Training

Initial training and regular retraining sessions should be planned for all employees who work in a network environment. Too often, "on the job training" really means no training at all. Under such circumstances, that users fail to understand their security responsibilities should come as no surprise.

Frequently, security programs are perceived negatively, as systems of restrictions and prohibitions.

Security officers are people who tell users what they cannot do, who make it harder to do the job. Security decisions seem to protect the system and the organization, without concern for the rights, needs, or efficiencies of the individual worker.

While security systems unavoidably include restrictive provisions, positive aspects should be emphasized. Encourage correct actions as well as prohibiting the incorrect. Stress the positive goals of the security program, goals with which all employees are generally in agreement. If people recognize security goals as their own, they will comply with security directives because doing so is in accord with their own individual interests.

Remember that security is as much psychology as technology. Perceptions are important. If people believe a system is secure, they will be less likely to attempt to circumvent it. If they feel a system is fair and sensible, they will be more willing to abide by its provisions. Training in the purposes behind security controls that apply to the group will go far in generating support for the system.

All users have to be brought into a peer group, otherwise peer influence is unlikely to affect them. Shared conferences and training brings computer users together; people of all ranks, from executives to clerks. By taking part in this type of orientation, users come to know the

trained and authorized users among them. Topics that should be discussed in these groups include:

- How user responsibilities as defined in the security policy statement affect the group and its area of concern.
- The workings of the information classification system and the special protective measures it provides.
- Reemphasize to employees that the company owns the information that it lawfully acquires and develops, and what the company expects the employee to do, or refrain from doing, in that regard.
- Remind employees of their obligation to protect the company's proprietary information, and that this is a condition of continued employment.
- Address infractions of the information security policy. Discuss the whole range of disciplinary measures from verbal warnings to dismissal. Examples of past infractions, and the disciplinary measures taken, can be effective.

Training sessions for users of a network are important. Specific explanations of expected procedures and behavior establish a security baseline. Reinforcement of ethical responsibilities can increase the likelihood that users behave in a security conscious manner.

D. SYSTEM IMPROVEMENT

The best way to deal with a security problem is to prevent it from happening. Many administrative practices can be used to head off security problems. These can be classified roughly as organizational, workplace, and personnel strategies (Kearby, 1990).

1. Organizational strategies

Large organizations frequently segregate, at least in function, those people who control:

- The mechanical parts of the system,
- The software that runs on it,
- The logical access structures, and
- The actual data input and output.

A typical organizational division is shown in Table 1.

Frequently Used Organizational Divisions of Control and Authority		
Level of Organization	DF Functions	Sample Job Titles
1	Control equipment and memory media	Computer Operators Tape Librarians
2	Write programs (control computer functions)	Systems Programmers Application Programmers
3	Control logical access and functions	Database Administrators
4	Control data input, modifications and output	Application Program User

Figure 1. Divisions of labor and authority

The idea behind this separation is to ensure that people who can access "live" data - end users - are restricted in what they are able to do to it, and those who can determine what may be done to data - programmers - have no access to real data. This structure makes it impossible to commit many types of fraud without collusion among two or more individuals, and thus reduces the likelihood that such crimes will be attempted or succeed if attempted.

A real danger today exists in organizations where microcomputers have a large role. While most mainframe operations are built around the division of labor because of the size of the jobs, most microcomputer operations are not. It is common to find one person acting as both programmer and computer operator. This same person may also maintain the tape and disk library, perform data input, and distribute the output.

This person has an inviting opportunity to commit fraud, steal from the organization, harm it severely with malicious actions against the computer, or hold information assets for ransom. Thus even in small organizations, the basic divisions should be pursued.

2. Workplace strategies

Today's workplace is that of the specialist. In small organizations particularly, this can pose a serious security threat. A single worker dedicated to a data processing function can commit errors or crimes without detection. The organization's dependence on that person can be disproportional to his actual value to the company.

Cross-training is an effective way to eliminate this threat. Every employee should be trained in some part of someone else's job. There should be no function that only one person can perform. By knowing the work process, employees will be able to perform spot checks on each others' work for quality control and audit purposes.

Problems also can be avoided by giving information only on a need-to-know basis. Confidential information should be distributed only to those who need it. An equally important corollary principle is not widely appreciated: If people do not have a need to know certain information, they also do not need to know it exists. Many information thefts could probably be avoided if the thieves were unaware the information was there to steal.

Minimize logon prompting. The more information an intruder must work to get, the more likely it is that he will give up the attempt to search for easier pickings.

The existence of significant assets should not be thrust into the public eye. Computer equipment and related activities should be inconspicuous. As a good example, newer computer facilities often are placed in windowless rooms, without any sign designating the activities carried on therein. This is an example of the principle of low profile.

Application of the principle of low profile is also appropriate to controls. It implies that the very existence of control measures may in fact be withheld from the subjects to whom the controls are applied. Alternatively, the details of how certain controls work may be withheld. Either of these approaches discourage attacks from knowledgeable insiders who might otherwise reason that they know how to defeat the controls. In general, it is a good idea to restrict access to documentation about controls.

Another asset control measure is to lower the user-to-terminal ratio. This will reduce the amount of time a terminal goes unattended, as well as ensure that fewer terminals are located in out of the way, hidden areas.

Another workplace strategy that can be effective is to have on-line access to sensitive information, rather than printed reports. This will upgrade security. There is no hard copy involved, retrieval time and individual productivity improve, and the electronic access provides a very detailed audit trail.

3. Personnel strategies

Accountability is a fundamental internal control principle, for information systems security and otherwise. It refers to a specific individual being answerable, responsible, or liable for specific activities. Thus, the use of a user-ID and a password as a means of identifying users on larger computers is instrumental in making such users accountable for the activities they perform on these computers. If mechanisms such as user-IDs and passwords did not exist, there would be no way of tracing specific activities to the initiating parties. Without such accountability, an audit would be impossible.

The operation of control measures should also be assigned to specific individuals. At least one individual should be explicitly accountable for the proper functioning of a control. The explicit assignment of this accountability is

very important in motivating involved parties to support specific control measures. For example, assigning accountability for the use of a specific user-ID to each individual is an important part of ensuring that the user does not share his password, choose a password that is easily guessed, or otherwise behave in a way that compromises the security provided by password-based access control packages.

To be able to assign accountability and responsibility to users, the users of the network must be validated. The security manager should formally verify the utilization of system resources by matching usernames and ID numbers against personnel file records. He should set up an automatic reporting routine that will identify accounts that have been unused for a specified period of time, as they may indicate employees that have moved or left the company.

Personnel strategies should focus on creating an atmosphere of personal responsibility and accountability within the user community. Training, rewards, and the certainty of punishment for wrongdoing can foster this atmosphere.

E. MAINTAINING SECURITY

All the methods previously described have as their ultimate aim the enhancement of security through the improvement of human factors in the organization. When these methods are implemented, security should improve. It is

important, however, not to neglect the system once the procedures have been put into place. Security managers must be vigilant in maintaining the environment they have worked to get.

Whether or not reality bears it out, an image of security and orderly operation should always be presented to the public and the user population. To look vulnerable is to invite attack and exploitation. From a systems design perspective, if an internal fault is detected, it should not be communicated to the users, but to an employee who is in a position to take corrective action. Some techniques to maintain a secure environment follow.

1. Employee accession

The success or failure of a security program depends on employee attitudes. Establishing the right security mindset is a process that should begin before an employee is hired and it should continue thereafter throughout his employment.

Interviews are often the most important determinant in hiring, but they are also among the least reliable and valid ways of selecting new employees. A resume carries only information the potential employee wants you to see, with no guarantee of validity and no hint of omissions. To the maximum extent possible, potential employees should be screened before they are hired. These are some useful screening techniques.

- Check references. Although organizations are reluctant to provide much information about their past employees these days, both firing for cause or prosecution for computer crime is likely to be revealed and will obviously be important information.
- Confirm background information. Many items on a resume can and should be confirmed. Aside from educational records, public records can be checked to rule out a criminal history.
- Examine work samples. Ask a person to provide samples of past work to demonstrate job-related skills as part of the job-consideration process. A programmer, for example, can be asked for copies of code and documentation written previously.

In short, do not trust the hiring decision to an interview and uncorroborated resume. The new employee who can fraudulently sell himself or herself into a new job may also be successful at computer fraud.

2. Hiring agreements.

These establish an understanding between employer and employee about expected standards of behavior. The hiring agreement must be closely coordinated to the organization's manual of policies and procedures. The agreement can be a part of the manual or can make specific reference to it.

Hiring agreements can be particularly useful for avoiding specific security threats. In a software house, for example, a hiring agreement can stipulate that rights to algorithms and software developed for the company, shall be the sole property of the employer. The hiring agreement sets expectations and a firm definition of right and wrong. Furthermore, unwillingness to sign such an agreement as a condition of hire might be an early warning of an employee who will not comply with security regulations.

3. Job descriptions

Information security should be an element of the job description. If a worker is expected to conform to security procedures, to be alert to and report possible security breaches, and to follow standards for quality assurance, these items should be included explicitly in the formal job description.

4. Punishment

The last resort for shaping employee behavior is disciplinary action. We hope that people will respond to positive incentives, and that disciplinary action will never be required. Nonetheless, discipline must be a part of the system.

Disciplinary action must be administered only when it is clearly deserved; the specific action should be decided upon before the event occurs. Disciplinary procedures that follow preset, published guidelines are exempt from such criticisms.

5. Functional cooperation

The data security officer should work to establish a close and cooperative relationship with the personnel department. Many of the security concerns discussed here are also good personnel practices for other reasons. Thus the security officer and the personnel director share many concerns and goals; working together, they can achieve results that would otherwise be out of reach.

6. System personalization

In computer crime, the fantasy of being invisible is as close to reality as it can be. In this sense, electronic information systems can make a perpetrator powerfully invisible. Unfortunately, not only is the perpetrator invisible, but often so is the victim. There is anonymity on both ends. This anonymity aids an intruder in setting aside any moral restraints that he might feel if the victim were personally known.

One way to decrease the sense of dealing with a machine is to personalize the system prompt. Upon requesting access to a sensitive application or data set, the prompt could be: "You are trying to access a restricted area, Joe, are you authorized for this?". The system has many attributes, but it lacks any kind of personal identity. Techniques similar to this can simulate an identity for the system, and promote a sense of ethical responsibility in the user.

7. System review

Information security plans must be regularly revisited and revised to reflect new technical developments and environmental changes. Security managers should be aware of new technological developments that can bring with them desirable human factors. Changes in the organizational environment must be monitored. If management shakeups result in an alteration of the human factors promoted within the

organization, security managers need to adjust controls to recognize that fact.

F. SUMMARY

Effective network security is not simply a function of elaborate technology. Tight security requires an integrated and concerted effort. The current security system must be evaluated in terms of its success in reaching defined security goals. Support for improvement must be gained from management and users. A comprehensive security plan, communicated to all concerned, will aid in gaining this support. Encouraging an ethical environment, and monitoring it, will maintain the security improvements and the enhanced security posture of the organization.

VII. CONCLUSIONS, RECOMMENDATIONS AND SUGGESTIONS FOR FUTURE RESEARCH

A. CONCLUSIONS

Human factors have a significant impact on the performance characteristics of network security control systems. The user of a control is an important component of the overall structure of security within an organization. Managers who ignore this interaction will find that security controls are a barrier to organizational efficiency and employee accomplishment.

The understanding and use of the human factors that impact network security leads to an environment conducive to information ethics, and the appropriate use of security controls. Use of a tool such as the Security Optimization Grid can aid in attaining such an environment.

The methods through which human factors are blended with security controls are not difficult. They merely require the attention of a security manager who is aware of the existence and importance of the human factors, the support of top-level management in the organization, and a program whereby the methods can be implemented and maintained.

To the question: What are the human factors that affect network security, the answers are:

- How closely the control is related to a similar user experience.

- The user's perception of how long the control takes to pass through.
- How much the user feels the control interferes with his routine.
- The degree to which the user feels the control is an invasion of his personal privacy.
- The speed and accuracy with which the control can be accomplished.
- The degree of involvement the user has in implementing the control.
- The amount of personal responsibility the user feels regarding the use of the control.
- Whether or not the user is rewarded for proper use of controls.
- The degree of management commitment to security controls.

To the question: How can a security manager utilize these factors to enhance security in his organization, the answers are:

- Do not force controls upon users
- Ensure controls are fast, and accurate.
- Ensure users are compensated if controls significantly interfere with their normal work routine.
- Involve users in the implementation of security controls.
- Ensure users perceive management's commitment to network security.
- Train users in their legal and moral responsibilities toward information systems in the organization.
- Reward users for good security practices.

B. RECOMMENDATIONS

Managers of networks carrying sensitive information should reevaluate their security controls systems with regard to human factors. Security measures currently in place were likely implemented without attention to those factors. An evaluation of the system with a tool such as the Security Optimization Grid may improve the operation of the current control methods.

Organizations with network information systems should attempt to create an atmosphere of ethical awareness as concerns the network. The ethical standards to which most people subscribe are based on human interaction. The absence of such ethical standards to apply to information systems can create problems in the network environment. The creation and fostering of an environment of information ethics will discourage misconduct in the network.

Future security control implementations should be made with human factors as a decision element of equal weight with technological advancement. The attitude of the involved user is important to the organization's effectiveness. If the user community feels neglected, or that its opinion is not valued, then they will attempt to bypass security controls. Additionally, their work performance, an critical issue for management, will degrade.

C. SUGGESTIONS FOR KEY RESEARCH

In the area of human factors as they affect network security, the current literature in the field generally lacks in-depth, analytical experimentation. Present studies focus on borderline intangibles such as user acceptance, satisfaction surveys, and the like. What is needed is experimental, quantified data.

For example, a study measuring the productivity of users before and after the implementation of some aspect of a human

factors program would be useful. It could show definitively if a positive correlation exists between human factors considerations and worker output.

Also of great significance would be an attempt to correlate the number of security violations in an organization with the particular atmosphere of human factors tolerance and the ethical environment. Such a correlation would provide concrete evidence that the areas are related, rather than relying on studies that can only infer user actions from similar circumstances and situations.

LIST OF REFERENCES

- Browne, Peter S., "How to Manage the Network Security Problem". *Computers and Security*, v. 3, pp. 77-87, 1990.
- Department of the Navy, OPNAVINST E239.1A, *The Department of the Navy ADP Security Program*, 1988.
- Haigh, Peter J., "Assuring Security with Distributed Micros". *Small Systems World*, v. 7, pp. 41-44, July 1984.
- Kearby, D'Ann B., "Personnel Policies, Procedures, & Practices -- The Key to Computer Security". *Computers and Security*, v. 4, pp. 63-68, 1990.
- Klopp, Charlotte. "Microcomputer Security Systems Attempt to Lock up Desktops". *Computers and Security*, v. 9, pp. 139-141, 1990.
- Klopp, Charlotte. "More Options for Physical Access Control". *Computers and Security*, v. 9, pp. 229-232, 1990.
- Leemah Systems. "Network Security at General Dynamics". *Telecommunication Products + Technology*, v. 4, pp. 66-68, February 1986.
- Menkus, Belden. "The Employee's Role in Protecting Information Assets". *Computers and Security*, v. 8, pp. 487-492, 1990.
- Oldehoeft, Arthur E., and David L. Jobusch. "A Survey of Password Mechanisms: Weaknesses and Potential Improvements. Part 2". *Computers and Security*, v. 8, pp. 675-689, 1990.
- Parker, Don B., "A Strategy for Preventing Program Theft and System Hacking". *Computers and Security*, v. 3, pp. 22-30, 1990.
- Pfleeger, Charles P., *Security in Computing*, pp. 387-392, Prentice Hall, 1989.
- Prause, Peter N., and Gerald I. Isaacson. "Protecting Personal Computers - A Checklist Approach". *Computer Security Journal*, v. 3, pp. 14-15, 1985.
- Sandia National Laboratories, *A Performance Evaluation of Biometric Identification Devices*, by James P. Holmes, Russell L. Maxwell, and Larry J. Wright, July 1990.

Secretary of the Navy Instruction, SECNAVNOTE 5230, ADP Control Guidelines, 1988.

SCAT '90, DEA and Biometrics, by Tony Antenucci, 1989.

Silverman, Martin E. "Selling Security to Senior Management, DP Personnel, and Users". *Computers and Security*, v. 2, pp. 7-14, 1990.

Shain, M. "Security in Electronic Funds Transfer". *Computers and Security*, v. 8, pp. 209-221, 1989.

Shaw, Elbert T. "Risk Analysis". Paper presented at NPGS, November 1988.

Sobol, Michael I. "Security Concerns in a Local Area Network Environment". *Telecommunications*, v. 3, pp. 96-102, March 1988.

Stoll, Clifford. *The Cuckoo's Egg*, Doubleday, 1989.

US Congress, *The Computer Security Act of 1987*, p. 2, Government Printing Office, Washington, DC, 1987.

Wood, Charles Cresson. "Principles of Secure Information Systems Design". *Computers and Security*, v. 9, pp. 13-24, 1990.

Y. j, Howard. "Hidden Troubles Plague Leaky Networks". *Telecommunication Products + Technology*, v. 3, pp. 26-34, June 1986.

Zimmerman, Joel S. "The Human Side of Computer Security". *Computer Security Journal*, v. 3, pp. 7-19, 1984.

Zviran, Moshe and James C. Hoge and Val A. Micucci. "SPAN - A DSS for Security Plan Analysis". *Computers and Security*, v. 9, pp. 153-160, 1990.

BIBLIOGRAPHY

Axner, David H. "Security Devices Prevent The Compromise of Network Resources". *Networking Management*, v. 2, February 1990.

Badenhorst, K.P. and Jan H.P. Eloff. "Framework of a Methodology for the Life Cycle of Computer Security in an Organization". *Computers and Security*, v. 8, 1989.

Bailey, Robert W. *Human Performance Engineering*, 2cd Ed., Prentice Hall, 1989.

Gardner, Phillip E. "Evaluation of Five Risk Assessment Programs". *Computers and Security*, v. 8, 1989.

Highland, Harold Joseph. "Random Bits & Bytes: The Premature Demise of Passwords". *Computers and Security*, v. 9, 1990.

Landreth, Bill. *Out of the Inner Circle*, Microsoft Press, 1985.

Moulton Rolf and Robert P. Bigelow. "Protecting Ownership of Proprietary Information". *Computers and Security*, v. 3, 1989.

Rothberg, Michael L. "Network Security: The Human Factor". *Computer Decisions*, v. 10, October 1988.

INITIAL DISTRIBUTION LIST

- | | | |
|----|---|---|
| 1. | Defense Technical Information Center
Cameron Station
Alexandria, Virginia, 22304-6145 | 2 |
| 2. | Superintendent
Attn: Library, Code 1424
Naval Postgraduate School
Monterey, California, 93943-5000 | 2 |
| 3. | Superintendent
Attn: Professor T.X. Bui, Code 036
Naval Postgraduate School
Monterey, California, 93943-5000 | 2 |
| 4. | Superintendent
Attn: LCDR R.L. Knight, Code 036
Naval Postgraduate School
Monterey, California, 93943-5000 | 2 |

**END
FILMED**

DATE:

12-91

DTIC